ユーザガイド - 日本語

FUJITSU Software ServerView Suite

ServerView 7.10 でのユーザ管理

中央認証と役割ベース認証

2015 年 5 月版

DIN EN ISO 9001:2008 に準拠した認証を取得

高い品質とお客様の使いやすさが常に確保されるように、
このマニュアルは、DIN EN ISO 9001:2008
基準の要件に準拠した品質管理システムの規定を
満たすように作成されました。

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

著作権および商標

出荷時期が変更される場合があります。技術的修正を施す権利を留保します。

目次

1　はじめに

このマニュアルでは、ServerView Suite および iRMC S2/S3/S4 のグローバルユーザ管理およびセキュリティアーキテクチャのベースとなる権限および認証のコンセプトについて説明します。

1.1　権限および認証のコンセプト

ServerView Suite および iRMC S2/S3/S4 のユーザ管理およびセキュリティアーキテクチャは、以下の 3 つの基本コンセプトがベースとなります。

– LDAP ディレクトリサービスを使用するグローバルユーザ管理
– 役割ベースのアクセス制御（RBAC）
– 中央認証サービス（CAS）に基づくシングルサインオン（SSO）

LDAP ディレクトリサービスを使用するグローバルユーザ管理

ユーザは、ディレクトリサービスにより、すべての関連する中央管理用サーバに対して一元的に保存および管理されます。ディレクトリサービスは、権限および認証に必要なすべてのデータを提供します。

ApacheDS や、すでに動作している設定済みのディレクトリサービス（Microsoft Active Directory など）などの、ServerView Operations Manager の固有の事前設定されているディレクトリサービスを使用するオプションがあります。

役割ベースのアクセス制御（RBAC）

役割ベースのアクセス制御（RBAC）では、一連のユーザ役割（セキュリティの役割）を定義することにより、アクセス制御を管理します。1 つまたは複数の役割を各ユーザに割り当て、1 つまたは複数のユーザ権限を各役割に割り当てます。

RBAC では、タスク指向の権限プロファイルを各役割に割り当てることにより、ユーザのセキュリティコンセプトとユーザの組織構造を連携させることができます。

RBAC は、ServerView Operations Manager のインストール時に自動的にインストールされる、ApacheDS ディレクトリサービスにすでに実装されています。Active Directory などのすでに設定されているディレクトリサービスを使

用する場合、そこに補足的に ServerView 固有の権限をインポートできます。続いて、関連する権限を持たせるユーザに必要な役割を割り当てることができます。

シングルサインオン（SSO）

ServerView Suite には、個々のコンポーネントにログインするためのシングルサインオン（SSO）機能があります。SSO は、中央認証サービス（CAS : **C**entral **A**uthentication Service）に基づいています。SSO では、一度だけユーザ認証を受ける必要があります。一度認証に成功すると、どのコンポーネントでもログインを再び要求されることなく、すべての ServerView コンポーネントにアクセスできます。

1.2　このマニュアルの対象ユーザ

本マニュアルの対象読者は、ハードウェアとソフトウェアの基本的な知識を有する、システム、ネットワーク管理者、サービス技術者です。このマニュアルでは ServerView Suite の権限および認証コンセプトの概要について紹介し、ServerView ユーザ管理のセットアップ手順、および ServerView ユーザ管理をユーザの IT 環境における既存のユーザ管理に統合する手順について詳しく説明します。

1.3 マニュアルの構造

このマニュアルでは、以下のトピックについて説明します。

- **第 2 章 : ユーザ管理およびセキュリティアーキテクチャ（概要）**

  この章では、ServerView Suite の権限および認証コンセプトの概要について紹介します。

- **第 3 章 : LDAP ディレクトリサービスを使用する ServerView ユーザ管理**

  この章では、以下のトピックについて説明します。

  – ディレクトリサービスアクセスの設定

  – ApacheDS を使用する ServerView ユーザ管理

  – ServerView ユーザ管理の Microsoft Active Directory への統合

- **第 4 章 : CMS および管理対象ノードでの SSL 証明書の管理**

  この章では、以下のトピックについて説明します。

  – SSL 証明書の管理（概要）

  – 集中管理サーバ（CMS）での SSL 証明書の管理

  – RBAC およびクライアント認証用の管理対象ノードの準備

- **第 5 章 : Operations Manager へのアクセスに関する役割ベースの許可**

  この章では、以下のトピックについて説明します。

  – 権限カテゴリと関連する権限

  – ApacheDS で事前定義されているユーザと役割

- **第 6 章 : 監査ログ**

  この章では、CAS 関連の監査ログ、監査ログの保管場所、監査ログエントリの構造についての詳細情報を説明します。

- **付録 1 : LDAP ディレクトリサービス経由の iRMC S2/S3 ユーザ管理**

  この章では、以下のトピックについて説明します。

  – iRMC S2/S3 によるグローバルユーザ管理の概念

  – ユーザ権限、権限グループ、役割

  – Microsoft Active Directory、Novell eDirectory、OpenLDAP、OpenDJ、OpenDS による iRMC S2/S3 ユーザ管理

- **付録 2 : LDAP ディレクトリサービス経由の iRMC S4 ユーザ管理**

  この章では、以下のトピックについて説明します。

  – iRMC S4 によるグローバルユーザ管理の概念

  – ユーザ権限、権限グループ、役割

  – Microsoft Active Directory、Novell eDirectory、OpenLDAP、OpenDJ、OpenDS、ApacheDS による iRMC S4 ユーザ管理

1.4 以前のマニュアルからの変更点

この版の『ServerView でのユーザ管理』マニュアルは、ServerView Operations Manager バージョン 7.10 に対応し、オンラインマニュアル『ServerView Suite - User Management in ServerView』（2014 年 03 月版）を置き換えるものです。

このマニュアルでは、以下の変更と追加について主に説明します。

- （OpenDJ の代わりに）ApacheDS を ServerView Operations Manager の「内部」ディレクトリサービスとして使用します。
- 新機能「統一 RBAC 管理」:

  「統一 RBAC 管理」では、ServerView Operations Manager（ApacheDS）の「内部」ディレクトリサービスを使用して役割の割り当てを管理し、「外部」ディレクトリサービス （Active Directory）にはユーザ認証の管理でのみアクセスします（27 ページ の「統一 RBAC 管理 :「外部」Active Directory による認証と「内部」ApacheDS による承認」の項を参照）。
- 事前定義されたユーザのパスワードを指定 / 変更する方法が変更されました（72 ページ の「LDAP バインドアカウントのパスワードの変更」の項を参照）。
- ServerView ユーザ管理 を Microsoft Active Directory に統合します（統一 RBAC 管理を使用するためのオプション）（63 ページ の「ServerView ユーザ管理の Microsoft Active Directory への統合」の項を参照）。

1.5 ServerView Suite リンクコレクション

ServerView Suite リンクコレクションにより、FUJITSU は ServerView Suite および PRIMERGY サーバに関するさまざまなダウンロードや詳細情報を提供します。

ServerView Suite には、以下のトピックに関するリンクがあります。

- サポートデスク
- マニュアル
- 製品情報
- セキュリティ情報
- ソフトウェアのダウンロード

ダウンロードには以下が含まれます。

– ServerView Suite の現在のソフトウェアバージョンおよびその他の Readme ファイル。

– ServerView Update Manager により PRIMERGY サーバをアップデートする場合、および ServerView Update Manager Express により個々のサーバをローカルでアップデートする場合の、システムソフトウェアコンポーネントの情報ファイルおよびアップデートセット。

– ServerView Suite のすべてのドキュメントの最新バージョン。

ダウンロードは FUJITSU Web サーバから無償で入手できます。

PRIMERGY サーバには、以下のトピックに関するリンクがあります。

- サポートデスク
- マニュアル
- 製品情報
- スペアカタログ

ServerView Suite リンク集へのアクセス

ServerView Suite のリンクコレクションへアクセスする方法はいくつかあります。

1. ServerView Operations Manager から。

   ► 開始ページまたはメニューバーで「**ヘルプ**」–「**リンク**」を選択します。

   ServerView Suite リンク集の開始ページが開きます。

2. FUJITSU マニュアルサーバで ServerView Suite のオンラインドキュメントの開始ページを使用する。

   i 次のリンクを使用して、オンラインドキュメントの開始ページにアクセスします。

   http://manuals.ts.fujitsu.com

   ► 左側の選択リストで「**x86 Servers**」を選択します。

   ► 右側で、「**Selected documents**」の「**PRIMERGY ServerView Links**」をクリックします。

   ServerView Suite リンク集の開始ページが開きます。

3. ServerView Suite DVD 2 から

   ► PRIMERGY ServerView Suite DVD 2 の開始ウィンドウで、「**ServerView Software Products**」を選択します。

   ► メニューバーで「**LINKS**」を選択します。

   ServerView Suite リンク集の開始ページが開きます。

1.6 ServerView Suite のマニュアル

マニュアルはインターネットからも無料でダウンロードできます。オンラインマニュアルは、*http://manuals.ts.fujitsu.com* の **x86 Servers** のリンク先からダウンロードできます。

ServerView Suite にあるドキュメントの概要およびファイル構造については、ServerView Suite サイトマップ（「**ServerView Suite**」- 「**Site Overview**」）を参照してください。

1.7 本ガイドの表記

このマニュアルでは以下の表記規則を使用します。

⚠ **注意**	このマークは、怪我、データ損失、装置破損に至る可能性のある危険性を示します。
i	この記号は重要な情報やヒントを強調しています。
►	このマークは、作業を続けるために行う必要のある手順を示します。
太字	説明文中の「**太字**」は、コマンド、メニュー項目、ボタン名、オプション、変数、ファイル名、およびパス名を示します。
固定幅フォント	システム出力は固定幅フォントを使用して示します。
太字の固定幅フォント	キーボードで入力する必要があるコマンドは、セミボールド固定幅フォントで示します。
<abc>	実際の値に置き換える変数を山括弧で囲みます。
[キーボードのキー]	キーボードの表示に従ってキーを示します。大文字での入力を明示的に示す場合は、Shift キーを併記します（例 : A の場合 [SHIFT] - [A]）。 2 つのキーを同時に押す場合は、2 つのキーをハイフンで連結して示します。

表 1: 表記規則

このマニュアル内のテキストまたはテキストの項への参照は、章または項の見出しと、章または項の開始ページで示します。

画面出力

画面出力は、使用するシステムに一部依存するため、細部がユーザのシステムに表示される出力と正確に一致しない場合があります。また、使用可能なメニュー項目がシステムによって異なる場合もあります。

2　ユーザ管理およびセキュリティアーキテクチャ（概要）

ServerView Suite のユーザ管理およびセキュリティアーキテクチャに提供される権限および認証のコンセプトは、以下の 3 つの基本コンセプトに基づいています。

– 19 ページ の「LDAP ディレクトリサービスを使用するグローバルユーザ管理」:

  ユーザ名は、ディレクトリサービスを使用して、すべての関連するプラットフォームに対して一元的に保存および管理されます。ディレクトリサービスは、権限および認証に必要なすべてのデータを提供します。

– 23 ページ の「役割ベースのアクセス制御（RBAC）」:

  役割ベースのアクセス制御（RBAC）では、ユーザ役割（セキュリティ役割）を使用して権限を割り当てることにより、ユーザ権限を管理します。この場合、各役割に固有のタスク指向の権限プロファイルを定義します。

– 30 ページ の「CAS サービスを使用するシングルサインオン（SSO）」:

  ServerView の各種製品には固有の Web サーバまたはアプリケーションサーバが搭載されており、このすべてが、管理者アクセスを許可する前に個別のユーザの ID を識別する必要があります。このため、ある製品の Web ページから別の製品の Web ページに変更するたびに、ユーザは自分の認証情報を指定する必要があります。

  SSO を使用する場合、一度ログインすると続いて「SSO ドメイン」に参加するすべてのシステムおよびサービスにアクセスでき、その各々に再びログインを要求されることはありません。「SSO ドメイン」は、同じ CAS サービスを使用して、認証を行うすべてのシステムで構成されます。

以降の項では、これらのコンセプトについてより詳しく説明します。

i　ServerView Operations Manager ≥ 5.0 と ServerView Agents < 5.0 との間のインタラクション :

ServerView Agents < V5.0 では上記のコンセプトをサポートしていません。それでも、ServerView Operations Manager V5.x を使用して ServerView Agents < V5.0 に対して任意の操作（セキュリティ関連の操作を含む）を実行できます。これを可能にするには、Operations Manager のユーザ / パスワードリストに、関連する管理対象ノードに対する有効なエントリ（適切な権限とユーザ / パスワードの組み合わ

せ）が含まれている必要があります。手順は、ServerView Operations Manager V5.0 以前で使用する手順と同様です。シングルサインオンはサポートしません。

2.1 前提条件

ServerView Suite ユーザ管理およびセキュリティアーキテクチャには以下のソフトウェアが必要です。

- JBoss Web サーバ

  バージョン 5.0 以降、ServerView Operations Manager では JBoss Web サーバを使用します。必要なファイルは ServerView Operations Manager software と共に自動的にインストールされます。

  JBoss は、**ServerView JBoss Applications Server 7** と呼ばれる独立したサービスとして設定します。サービスは次の方法で開始 / 停止できます。

  – Windows Server 2008/2012 システムの場合 :

  「管理ツール」-「サービス」を選択します

  すべての Windows システムで、次の CLI コマンドを使用して JBoss サービスを開始 / 停止することもできます。

```
"%WINDIR%\system32\net.exe" start "ServerView JBoss Application Server 7"
```

```
"%WINDIR%\system32\net.exe" stop "ServerView JBoss Application Server 7"
```

  – Linux システムの場合、次のコマンドを使用します。

```
/etc/init.d/sv_jboss start|stop
```

- LDAP ディレクトリサービス

  ServerView Operations Manager のインストール時に、ServerView Operations Manager の内部で使用される ApacheDS ディレクトリサービスを使用するか、既存のディレクトリサービス（Microsoft Active Directory など）を使用するかを選択できます。

- 中央認証サービス（CAS）

  シングルサインオン（SSO）機能には CAS サービスが必要です。CAS サービスはユーザ認証情報をサーバ側にキャッシュし、ユーザが異なるサービスを要求すると、ユーザに認識されない方法でユーザ認証を行います。

  CAS は ServerView Operations Manager ソフトウェアと共に自動的にインストールされます。

上記コンポーネントを含む ServerView Operations Manager のインストール方法については、『ServerView Operations Manager - Installation under Windows』および『ServerView Operations Manager - Installation under Linux』を参照してください。

2.2 LDAP ディレクトリサービスを使用するグローバルユーザ管理

ServerView Suite および iRMC S2/S3/S4 のグローバルユーザ管理ではそれぞれ、すべての中央管理用サーバ（CMS）/ iRMC S2/S3/S4 のユーザを LDAP ディレクトリサービスのディレクトリに一元的に保存します。これにより、ユーザを中央サーバで管理することができます。そのため、これらのユーザは、このサーバに接続されるネットワーク上のすべての CMS および iRMC S2/S3/S4 で使用できます。

i **注意事項 :**

統合ユーザ管理を共通ディレクトリサービスに基づいて実行することは、iRMC S2/S3/S4 が **DEFAULT** 部門に属するように設定されている場合にのみ、ServerView ユーザとグローバル iRMC S2/S3/S4 ユーザの両方に対して機能します。

i このマニュアルを通して、「iRMC S2/S3/S4 のユーザ管理」は「グローバル」iRMC S2/S3/S4 ユーザ管理という意味で使用されます。また、iRMC S2/S3/S4 は「ローカル」ユーザ管理をサポートします。これは関連するユーザ ID を iRMC S2/S3/S4 の不揮発性記憶装置にローカルに保存し、iRMC S2/S3/S4 ユーザインターフェースで管理します（詳細は『iRMC S2/S3 - integrated Remote Management Controller』および『iRMC S4 - integrated Remote Management Controller』マニュアルを参照）。

2.2.1 ディレクトリサービスを使用する利点

ディレクトリサービスを使用することで、次の利点を得られます。

– ディレクトリサービスは実際のユーザ ID を管理し、一定しないローカルアカウントではなく、個人 ID を使用できるようにします。

– ディレクトリサービスはユーザ管理をサーバ管理から切り離します。このため、サーバ管理者はディレクトリサービスデータを変更する権限がなければ、ユーザ権限を変更できません。

ServerView はユーザの認証と権限の両方にディレクトリサービスを使用します。

– 認証（Authentication）ではユーザの ID を検証します : ユーザが「**誰**」であるか。

– 承認（Authorization）ではユーザの権限を定義します : ユーザに「**何**」を許可するか。

また、CMS のディレクトリサービスを使用すると、同じユーザ ID で CMS および管理対象サーバにログオンできます。

2.2.2 サポートするディレクトリサービス

ServerView Suite でサポートされるディレクトリサービス

ServerView Suite は現在、以下のディレクトリサービスをサポートしています。

– ApacheDS
– Microsoft Active Directory

i ServerView Operations Manager のインストール時には、ServerView の内部ディレクトリサービス（ApacheDS）を選択するオプションがあります。

iRMC S2/S3/S4 でサポートされるディレクトリサービス

iRMC S2/S3/S4 は現在、以下のディレクトリサービスをサポートしています。

– Microsoft Active Directory
– Novell eDirectory
– OpenLDAP[OpenLDAP]
– ApacheDS

2.2.3 ApacheDS または既存の設定済みディレクトリサービスの使用

Using ApacheDS

Operations Manager のインストール時に別のディレクトリサービスを指定しなければ、セットアップ時に Using ApacheDS が固有のディレクトリサービスとしてインストールされます。そのため、Using ApacheDS は **ServerView JBoss Application Server 7** サービスが実行中の場合にのみ使用できます。

既存の設定済みディレクトリサービスの使用

ユーザの IT 環境でディレクトリサービス（Microsoft Active Directory）がすでにユーザ管理に割り当てられている場合、それを ServerView 固有の ApacheDS の代わりに使用できます。

2.2.4 ServerView Suite および iRMC S2/S3/S4 用の Common User Management

Active Directory を使用して、ServerView Suite と関連する iRMC S2/S3/S4 で管理されるすべてのサーバからなる、多部門サーバユーザ管理を設定できます。

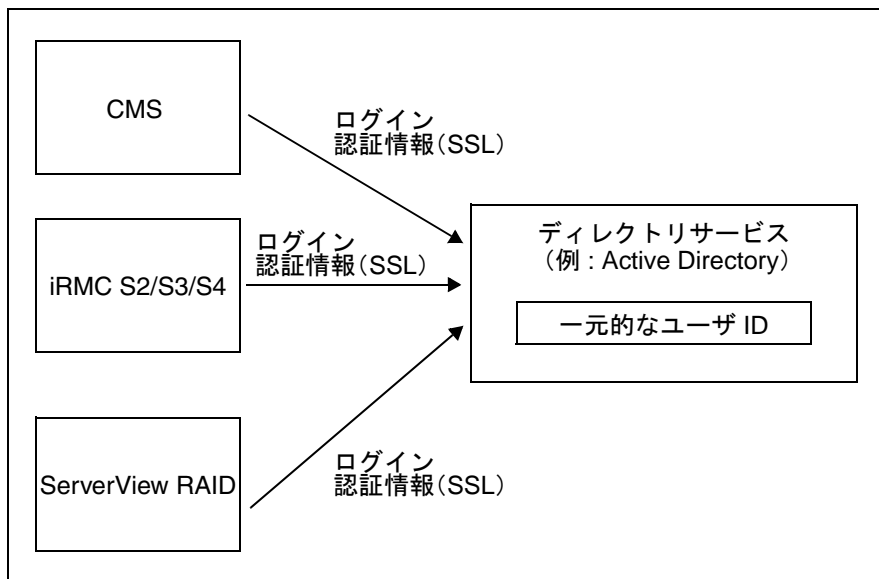



図 1: ServerView Suite のさまざまなコンポーネントでのグローバルユーザの共用

個々の CMS / iRMC S2/S3/S4 などと中央ディレクトリサービスとの間の通信は、TCP/IP プロトコル LDAP（**L**ightweight **D**irectory **A**ccess Protocol）を使用して行われます。LDAP では、最も頻繁に使用されるディレクトリサービスおよびユーザ管理に最も適したディレクトリサービスにアクセスできます。

セキュリティ上の理由のため、LDAP での通信は SSL で保護してください。SSL で保護しない場合、パスワードはプレーンテキストで送信されます。

2.3 役割ベースのアクセス制御（RBAC）

ServerView Suite のユーザ管理およびグローバル iRMC S2/S3/S4 ユーザ管理は役割ベースのアクセス制御（RBAC）に基づいているため、ユーザのセキュリティコンセプトをユーザの組織構造に適応させることができます。

RBAC は権限最小の原理に基づいています。これは、特定の ServerView コンポーネントの使用、または特定の ServerView 固有のタスクの実行について、必要以上の権限をユーザに付与しないということです。

2.3.1 ユーザ、ユーザ役割、権限

RBAC では、ユーザに対応する権限を直接割り当てる代わりに、ユーザ役割を使用してユーザへの権限の割り当てを制御します。

– 一連の権限が各ユーザ役割に割り当てられます。各権限セットでは、ServerView Suite のアクティビティにタスク指向の権限プロファイルを定義します。

– 1 つまたは複数の役割が各ユーザに割り当てられます。

ユーザロールの概念には、以下のような重要な利点があります。

– 各々のユーザまたはユーザグループに、個別に許可を割り当てる必要がない。その代わりに、許可はユーザロールに従って割り当てられる。

– 権限の構造が変更された場合のみ、権限をユーザ役割に適応させることが必要です。

各ユーザに複数の役割を割り当てることができます。この場合、このユーザへの権限は、割り当てられたすべての役割の権限を組み合わせて定義されます。

2.3.2 ApacheDS での RBAC の実装

RBAC は、Operations Manager のインストール時に自動的にインストールされる、ApacheDS ディレクトリサービスにすでに実装されています。

事前定義されているユーザおよび役割

デフォルトでは、ApacheDS には事前定義されたユーザ役割 **Administrator**、**Monitor**、Operator、**UserAdministrator** があり、それぞれ事前定義されたユーザ **Administrator**、**Monitor**、Operator、**UserManager** 専用です。ユーザ、役割、役割とユーザとの割り当てを追加作成して、セキュリティコンセプトを組織の構造に合わせることもできます。

図 2 に、ユーザ名 **Administrator**、**Monitor, Operator**、**UserManager** と、対応する役割 **Administrator**、**Monitor**、**Operator**、**UserAdministrator** を使用する、役割ベースの割り当てコンセプトを示します。

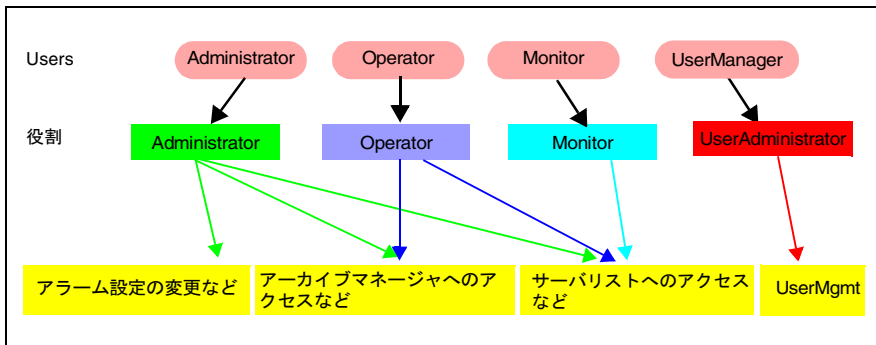



図 2: 役割ベースのユーザ権限の割り当て例

厳密には、ApacheDS は特定の目的専用に許可される 2 つのユーザを事前定義します。
"cn=system administrator"（ApacheDS の Directory Superuser）と **svuser**（CAS および ServerView のセキュリティモジュールがディレクトリサービスにアクセスするために使用）です。

既定のユーザ役割によって付与される権限の範囲は、低い方から **Monitor**（最低許可レベル）、**Operator**、**Administrator**（最高許可レベル）です。詳細は、127 ページ の「監査ログ」の章を参照してください。

> **i** 役割 **UserAdministrator** はこの階層に当てはまりません。ApacheDS によるユーザ管理を可能にする権限を付与することのみを目的としているためです。外部ディレクトリサービス（Active Directory など）を ServerView のユーザ管理に使用している場合、**UserAdministrator** 役割はこのディレクトリサービスにインポートされません。

セキュリティコンセプトの組織構造への適応

セキュリティコンセプトを組織構造に適応させるため、ServerView Suite では、SerververView Operations Manager のスタートページにある「**セキュリティ**」エントリの「**ユーザ管理**」リンクを使用して、追加のユーザ、役割、役割とユーザの割り当てを簡単に作成できます。

2.3.3 既存の設定済みディレクトリサービスと RBAC との連携

ServerView Suite の RBAC ユーザ管理を、設定済みの「外部」ディレクトリサービス（Microsoft Active Directory など）に基づく既存の RBAC ユーザ管理に統合することもできます。詳細は、63 ページ の「ServerView ユーザ管理の Microsoft Active Directory への統合」の項を参照してください。

この場合、ServerView のユーザおよびセキュリティコンセプトでは次のオプションを提供します。

– ユーザ認証とユーザ承認は、同じ「外部」ディレクトリサービス（Active Directory など）で管理します。

– 「統一 RBAC 管理」では、ServerView Operations Manager（ApacheDS）の「内部」ディレクトリサービスを使用して役割の割り当てを管理し、「外部」ディレクトリサービス （Active Directory）にはユーザ認証の管理でのみアクセスします。

> **i** ServerView Operations Manager のインストール時に、上記戦略のどれを ServerView ユーザ管理に使用するか指定できます。統一 RBAC 管理の場合は、「外部」ディレクトリサービスのドメイン名の入力が求められます。このドメイン名により、後で Central Authentication Service へのログイン時に、適切な認証ドメインを選択できます。

2.3.3.1 Active Directory 内の認証と承認

このアプローチは、一貫性のある認証および承認の集中管理を提供するという優位性があります。一方、社内の Active Directory を使用して ServerView Operations Manager を構成するには、権限、役割、部門の宣言といった ServerView ユーザ管理の承認データを、社員のユーザアカウントが保存されるドメインコントローラにインポートする必要があります。このような LDIF インポートは、セキュリティ上の理由により多くの IT 管理者から批判的に見られています。

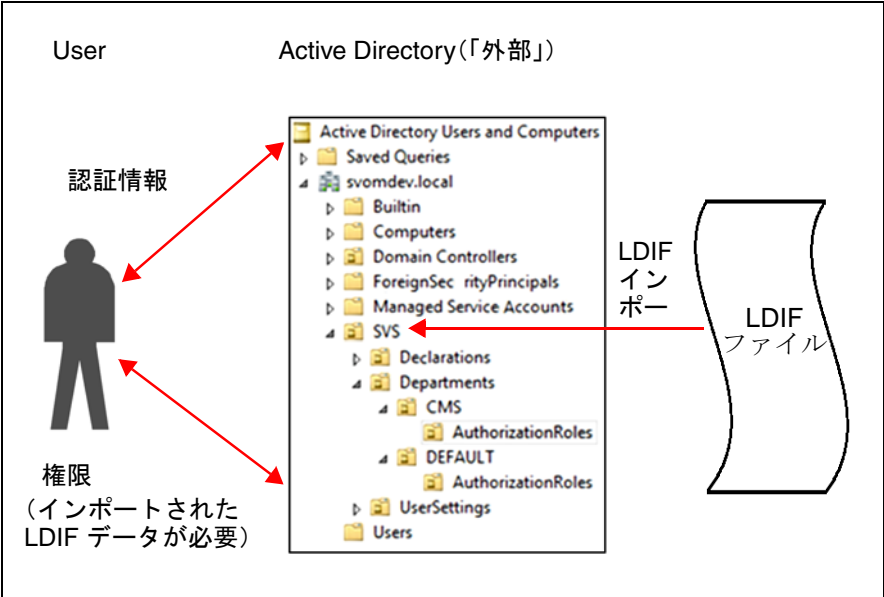



図 3: 同じ外部ディレクトリサービス内の認証と承認

図 3 では、ユーザの認証と承認の両方が Active Directory で実行され、LDIF から事前にインポートしたデータと、ユーザの役割を割り当てるために作成したデータを使用できます。

2.3.3.2 統一 RBAC 管理：「外部」Active Directory による認証と「内部」ApacheDS による承認

統一 RBAC 管理では、ユーザ承認データの LDIF インポートとそれに関連するセキュリティ問題を回避することができます。

– ServerView Operations Manager の「内部」ディレクトリサービス（ApacheDS）が、ユーザへの役割の割り当てに常に使用されます。

– 「外部」ディレクトリサービス（Active Directory）は、ユーザ承認を目的としてのみアクセスされます。

そのため、統一 RBAC 管理の手法は、「外部」ディレクトリサービス（Active Directory など）を使用する場合にのみ推奨されます。

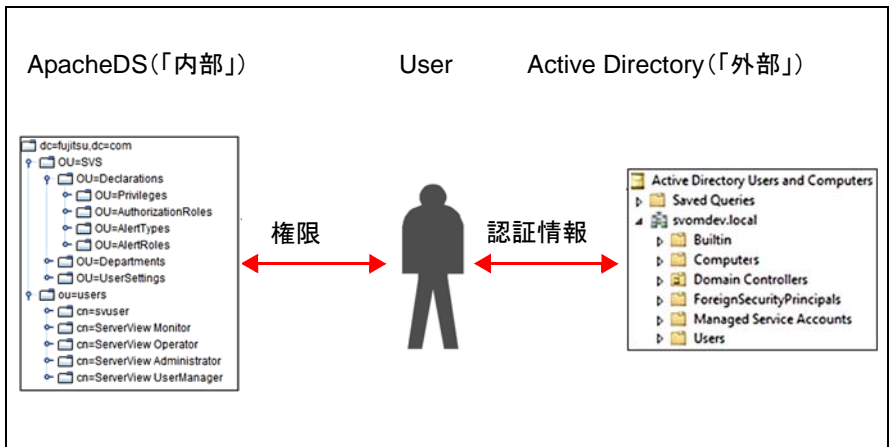



図 4: 「外部」Active Directory による認証と「内部」ApacheDS による承認

統一 RBAC 管理を構成すると以下のようになります。

- Central Authentication Service のログインウィンドウで、ユーザアカウントの認証ドメインを指定するように求められます（『ServerView Operations Manager』マニュアルを参照）：

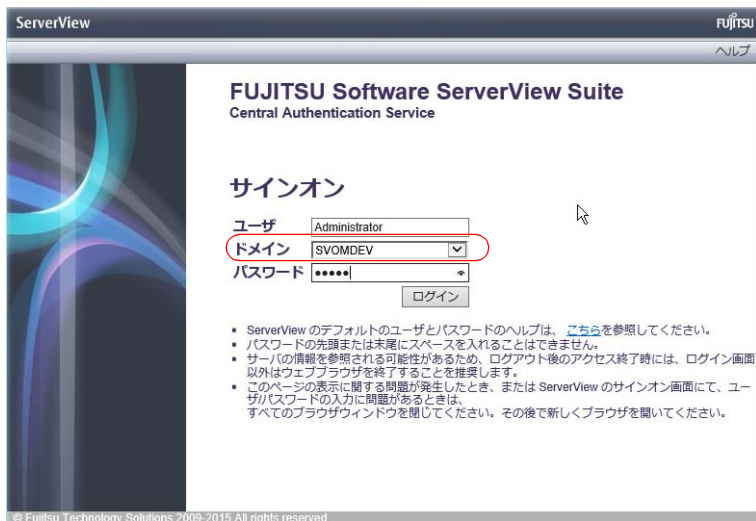



図 5: CAS ログインウィンドウ

- **「ユーザ管理」**ウィザードの**「ロール割り当て」**ダイアログボックスで、ユーザを表示する欄が 2 つのサブ欄に分かれます（詳細は、**「Operations Manager - ユーザ管理」**オンラインヘルプを参照）：

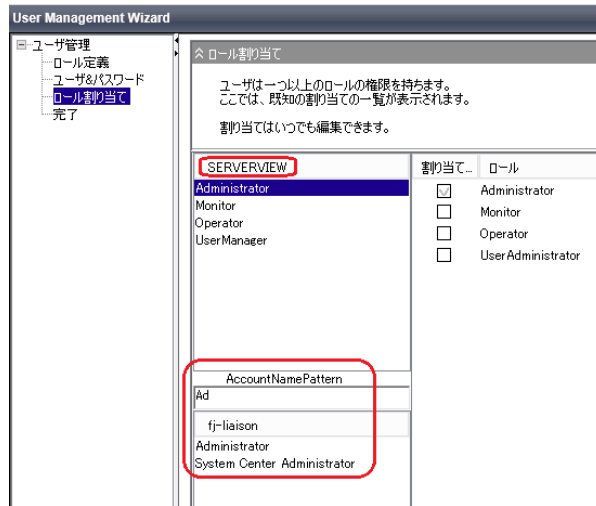



図 6: 「ユーザ管理」ウィザード - 「ロール割り当て」（統一 RBAC 管理が構成されている）

– 上のサブ欄には、ApacheDS（ドメイン **SERVERVIEW**）で管理されるユーザが表示されます。

– 下のサブ欄には、「外部」ディレクトリサービス（Active Directory など、ServerView Operations Manager のインストール時に指定されるドメイン）で管理されるユーザが表示されます。

2.4 CAS サービスを使用するシングルサインオン（SSO）

ユーザが個々のコンポーネント（Web サービスなど）にログインできるように、ServerView Suite にはシングルサインオン（SSO）機能があります。ServerView では、中央認証サービス（CAS）を使用して SSO メカニズムを実装し、ユーザからは完全に見えない形で、シングルサインオン手順を処理します。

重要！

PC の前を離れるときは、必ずサインオフしてブラウザを閉じてください。

CAS はユーザの ID 情報をセキュアなブラウザ Cookie（チケット認可 Cookie（TGC）、32 ページを参照）に保存します。これは、ユーザが明示的にサインオフしたとき、またはユーザがブラウザを閉じたときに削除されます。このため、ブラウザセッションを放置すると重大なセキュリティ問題が発生します。

SSO を使用するための要件

– CAS サービスを、SSO ドメインに参加しているすべての iRMC S2/S3/S4 に対して設定する必要があります（詳細は『iRMC S2/S3 - integrated Remote Management Controller』および『iRMC S4 - integrated Remote Management Controller』マニュアルを参照）。

– SSO ドメインに参加するすべてのシステムは、同じ IP アドレス表記を使用して CMS を参照することが必須です。（「SSO ドメイン」は、同じ CAS サービスを使用して、認証を行うすべてのシステムで構成されます。）そのため、たとえば「my-cms.my-domain」という名前を使用して ServerView Operations Manager をインストールした場合、これとまったく同じ名前を使用して iRMC S2/S3/S4 の CAS サービスを指定します。そうせずに、「my-cms」のみや my-cms の別の IP アドレスを指定しても、SSO は 2 つのシステム間で有効になりません。

2.4.1 CAS ベースの SSO アーキテクチャ

SSO アーキテクチャは以下のコンポーネントとアイテムに基づいています。

– 中央認証サービスを提供する CAS サービス

– CAS 可能な（「CAS 化された」）任意の ServerView Suite コンポーネントの一部としての CAS クライアント

– サービスチケット（ST : Service Ticket）

– チケット認可チケット（TGT : Ticket Granting Ticket）

中央認証サービス（CAS サービス）によるユーザ認証の管理

CAS サービスは中央ユーザ認証を管理します。この場合、CAS サービスは、管理コンソール（クライアントシステム）のブラウザと、ユーザを管理するディレクトリサービスを仲介します。

CAS クライアントによるサービス要求の切断およびリダイレクト

CAS クライアントは、「CAS される」任意の ServerView Suite コンポーネントの一部で、ユーザ認証を有効にするためにコンポーネントへの任意の要求を切断するフィルタです。CAS クライアントはこの要求を CAS サービスにリダイレクトし、続いて CAS サービスがユーザ認証を処理します。

サービスチケット（ST）およびチケット認可チケット（TGT）

ユーザの認証が成功すると、CAS サービスはいわゆるチケット認可チケット（TGT）をユーザに割り当てます。これは技術的に、対応するセキュアなブラウザ Cookie を設定することにより実現します。ServerView Suite コンポーネントの CAS クライアントが HTTPS 要求を CAS サービスにリダイレクトすると必ず、TGT Cookie によってサービスが要求固有のサービスチケット（ST）を作成し、それを、追加の要求パラメータを使用して CAS クライアントに返します。CAS クライアントは最初に CAS サービスを直接呼び出して ST を有効にし、次にオリジナルの要求を ServerView Suite コンポーネントに渡します。

チケット認可 Cookie（TGC : Ticket Granting Cookie）

Web ブラウザは、CAS サービスとの SSO セッションを確立すると、セキュアな Cookie を CAS サービスに提供します。この Cookie にはチケット認可チケット（TGT）が含まれているため、チケット認可 Cookie（TGT Cookie または TGC）と呼ばれます。

i TGC は、ユーザが CAS をログアウトするかブラウザを閉じると破棄されます。チケット認可チケット Cookie には有効期間があり、CAS サービスのコンフィグレーションファイルに設定されます（事前設定値 : 24 時間）。有効期間は最大 24 時間です。つまり、ユーザは最長 24 時間後にログアウトされます。この最大時間は、インストールされているシステムで変更することはできません。

CAS ベースの SSO が初期のシングルサインオン（SSO）要求を処理する方法

図 7 に、CAS ベースのシングルサインオン（SSO）が初期のシングルサインオン認証を処理する方法を示します。

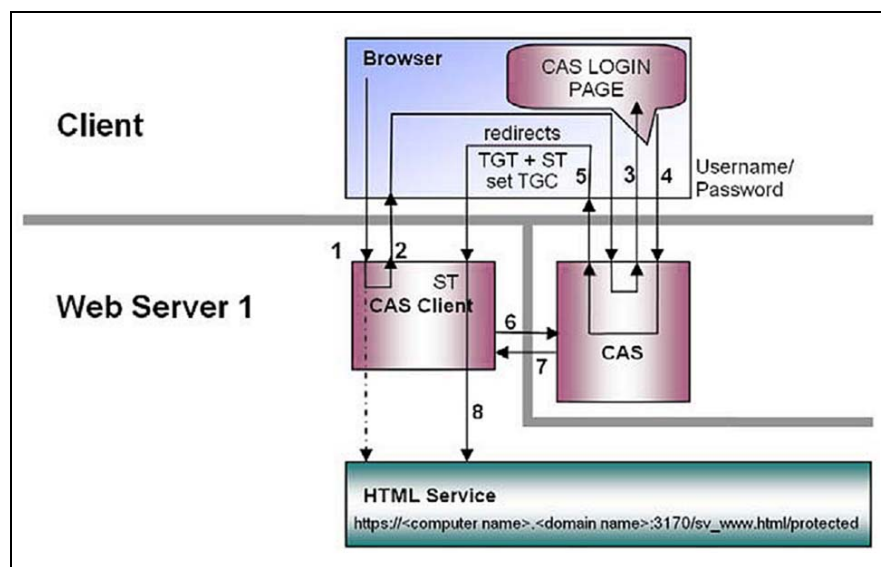



図 7: CAS サービスを使用する SSO アーキテクチャ

説明

1. ユーザは管理コンソールにサービスの URL を入力し、Operations Manager などの ServerView Suite コンポーネントを呼び出します。
2. このユーザ要求は、CAS サービスにリダイレクトされます。
3. CAS サービスは CAS ログインウィンドウを生成し、管理コンソールに表示されます。CAS ログインウィンドウは、ユーザにログイン認証情報（ユーザ名およびパスワード）を要求します。
4. ユーザはログイン認証情報を入力します。
5. CAS サービスはユーザ名およびパスワードを認証し、要求を要求元のコンポーネントにリダイレクトします。また、CAS サービスは TGT Cookie を設定し、ユーザにサービスチケット（ST）およびチケット認可チケット（TGT）を割り当てます。
6. CAS クライアントはサービスチケットを CAS サービスに送信し、検証を要求します。
7. 検証に成功した場合、CAS サービスは、「Service Ticket is ok」という情報とユーザ名を返します。
8. Web アプリケーション（ServerView コンポーネント）はオリジナルの要求に応答します（ステップ 1 を参照）。

CAS ベースの SSO が後続の SSO 要求を処理する方法

サービス（Operations Manager など）へのアクセス認証に成功すると、ログイン認証情報を要求されることなく、ユーザは別のサービス（iRMC S2/S3/S4 Web インターフェースなど）を呼び出すことができます。この場合、CAS サービスは、このユーザが前のログイン手順で設定したチケット認可 Cookie（TGC）を使用して認証を行います。

この TGC が有効なチケット認可 Cookie（TGC）と一致する場合、Web ブラウザが「SSO ドメイン」のサービスに要求を送信するたびに、CAS サービスが自動的にサービスチケット（ST）を発行します。そのため、ユーザは認証情報を要求されずに ServerView Suite コンポーネントにアクセスできます。

2.4.2 ユーザから見たシングルサインオン

SSO では、ユーザが CAS サーバに認証を証明する必要があるのは一度だけです。初めて ServerView Suite コンポーネント（Operations Manager など）にログインすると、CAS サービスによって、ユーザの認証情報（ユーザ名およびパスワード）を要求する別のウィンドウが表示されます。一度認証に成功すると、どのコンポーネントや iRMC S2/S3/S4 でもログインを再び要求されることなく、SSO ドメインのすべての ServerView Suite コンポーネントおよび iRMC S2/S3/S4 にアクセスできます。

(1)ユーザが HTTP 要求を ServerView Suite コンポーネントに送信します。

(1a)CAS はこの要求を CAS サービスに内部的にリダイレクトします（ユーザには見えません）。

(2)CAS サービスが、ユーザにログイン認証情報を要求するログインウィンドウを表示します。

(3)ユーザがユーザ名とパスワードを入力し、ユーザの設定を確定します。

(4)CAS サービスがこのユーザを認証します。

(5)一度認証に成功すると、再びログインを要求されることなく、ユーザは他のコンポーネントにもアクセスできます。

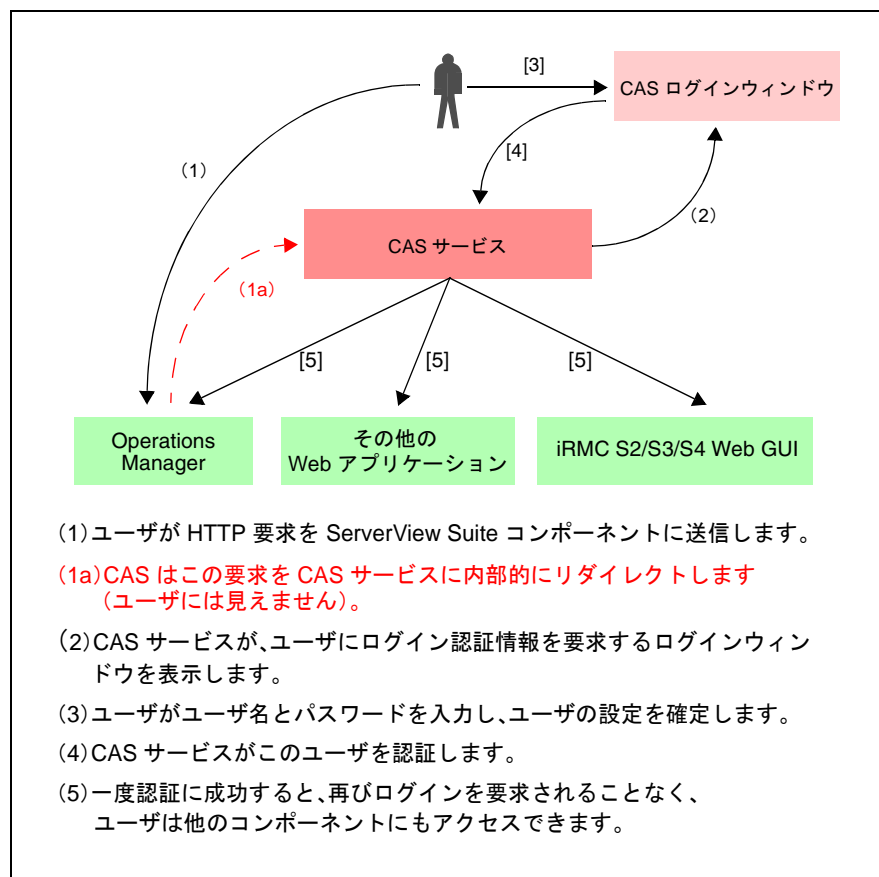



図 8: ユーザから見たシングルサインオンの手順

3　LDAP ディレクトリサービスを使用する ServerView ユーザ管理

この章では、以下のトピックについて説明します。

– 35 ページ の「ディレクトリサービスアクセスの設定」
– 36 ページ の「ApacheDS を使用する ServerView ユーザ管理」
– 63 ページ の「ServerView ユーザ管理の Microsoft Active Directory への統合」

注意事項 :

ServerView ユーザ管理と iRMC S2/S3/S4 グローバルユーザ管理の両方を同じ組織単位（OU）**SVS** で動作させるには、iRMC S2/S3/S4 ユーザ管理が **DEFAULT** 部門のみを使用する必要があります。

警告ロールは ServerView Suite では使用できないため、iRMC S2/S3/S4 以外のすべての ServerView コンポーネントで無視されます。

3.1　ディレクトリサービスアクセスの設定

ServerView ユーザ管理の中央認証と役割ベース認証は、どちらも LDAP ディレクトリサービスを使用して一元管理されるデータに基づいて行われます。Operations Manager セットアップ中に、LDAP ディレクトリサービスへの接続に必要な情報が要求されます。

この設定を後で変更する場合は、次の手順に従います。

– Windows システムでは、アップグレード / 変更インストールを実行するセットアップを繰り返します。

– Linux システムでは、次のコマンドを実行します。
/opt/fujitsu/ServerViewSuite/svom/ServerView/Tools/ChangeComputerDetails.sh

3.2 ApacheDS を使用する ServerView ユーザ管理

ServerView Operations Manager のインストール時に別のディレクトリサービスを指定しなければ、セットアップ時に ApacheDS が固有のディレクトリサービスとしてインストールされます。詳細は、『Installing ServerView Operations Manager Software under Windows』および『Installing ServerView Operations Manager Software under Linux』マニュアルを参照してください。

3.2.1 事前定義されているユーザおよび役割

役割ベースのアクセス制御（RBAC）は、ApacheDS ディレクトリサービスにすでに実装されています。ApacheDS にはユーザ役割の **Administrator**、**Monitor**、Operator、**UserAdministrator** が事前定義されており、事前定義されたユーザの **Administrator**、**Operator**、**Monitor**、**UserManager** にそれぞれ専用に割り当てられます。また、ApacheDS には、特別な目的専用の、完全に権限が付与されている 2 つのユーザが事前定義されます。

37 ページ の表 2 に、ApacheDS に事前定義されるユーザ名、パスワード、および役割を示します。

注意！

セキュリティを向上させるために、できるだけ早く事前定義されたパスワードを変更してください。パスワードの変更方法の詳細は、38 ページ の「事前定義されたユーザのパスワードの定義 / 変更」の項を参照してください。

個々のユーザ役割に付与される権限の範囲の詳細は、109 ページ の「Operations Manager へのアクセスに関する役割ベースの許可」の章を参照してください。

名前	パスワード	ユーザ役割	LDAP 識別名 / 説明
./.	admin		cn=Directory Manager、cn=RootDNS、cn=config これは、ApacheDS の Directory Manager アカウントです。ルート DN（ルートユーザ）には通常、サーバのすべてのデータへのフルアクセスが付与されます。ApacheDS では、ルートユーザはアクセス制御評価をデフォルトでバイパスできるようになります。ルートユーザはサーバ設定にフルアクセスでき、他のほとんどのタイプの操作を行います。 ApacheDS では、サーバを複数のルートユーザで設定できます。ルートユーザに付与されるすべての権利は、権限を通じて割り当てられます。
svuser	ServerView Operations Manager のインストール中にパスワードを指定する必要があります。		cn=svuser,ou=users,dc=fujitsu,dc=com このアカウントを使用して、CAS および ServerView のセキュリティモジュールを使用してディレクトリサービスにアクセスします。以下のコンフィグレーションファイルに、関連するデータがあります。 **<ServerView directory>\jboss\standalone\svconf\sv-sec-config.xm**
Administrator	admin	Administrator	Administrator 役割のデフォルトユーザ。
モニタ	admin	モニタ	Monitor 役割のデフォルトユーザ。
Operator	admin	Operator	Operator 役割のデフォルトユーザ。
UserManager	admin	UserAdministrator	UserAdministrator 役割のデフォルトユーザ。

表 2: ApacheDS に事前定義されるユーザ名、パスワード、および役割

3.2.2 事前定義されたユーザのパスワードの定義 / 変更

注意事項 :

パスワードにはバックスラッシュ（＼）、円記号（￥）を使用しないでください。

3.2.2.1 ApacheDS Directory Manager のパスワード

なお、次の点に注意してください。

ApacheDS Directory Manager の事前定義されたパスワードは「admin」です。セキュリティ上の理由から、事前定義されたパスワードを変更することを強く推奨します。

以下の説明では、文字列 "new_dm_pw" は、新しいパスワードのプレースホルダです。プレースホルダを、使用する適切なパスワードに置き換えてください。

Windows システムでの ApacheDS Directory Manager の事前定義されたパスワードの変更

なお、次の点に注意してください。

パーセント記号（%）を 1 つ以上含むパスワードを設定するには、コマンドラインでパスワードを指定するときに、パーセント記号を二重にする必要があります。たとえば、コマンドラインで `hello%%world` と入力すると `hello%world` というパスワードを設定できます。

Windows システムの場合、次の手順に従って事前定義されたパスワードを変更します。

1. Windows コマンドプロンプトを開きます。
2. ディレクトリを **<ServerView ディレクトリ >\apacheds\bin** に変更します。

3. 次のコマンドを 1 行で入力して、ApacheDS Directory Manager のパスワード（ここでは、事前定義されたパスワード「admin」）を変更します。

```
ldappasswd -H ldap://localhost:1473 -D
"uid=admin,ou=system" -w "admin" -s "new_dm_pw"
"uid=admin,ou=system"
```

> **i** このコマンドを実行すると、「ber_scanf: No such file or directory」というメッセージが表示されます。このメッセージは無視してください。

Linux システムでの ApacheDS Directory Manager の事前定義されたパスワードの変更

> **i** **なお、次の点に注意してください。**
>
> シェルの特殊文字を 1 つ以上含むパスワードを設定するには、コマンドラインでパスワードを指定するときに、バックスラッシュを特殊文字の前に置いてエスケープする必要があります。たとえば、コマンドラインで `hello\$world` と入力すると `hello$world` というパスワードを設定できます。

Linux システムの場合、次の手順に従って事前定義されたパスワードを変更します。

1. コマンドシェルを開きます。
2. 次のコマンドを 1 行で入力して、ApacheDS Directory Manager のパスワードを変更します。

```
ldappasswd -H ldap://localhost:1473 -D
"uid=admin,ou=system" -w "admin" -s "new_dm_pw"
"uid=admin,ou=system"
```

3.2.2.2 svuser のパスワードの定義 / 変更

ServerView Operations Manager のインストール中に、管理者ユーザ「**svuser**」が ApacheDS データベース内に作成されます。

svuser のパスワードに空白の文字列は指定できません。

Windows システムでの svuser のパスワードの定義 / 変更

ServerView Operations Manager のセットアップ中に、まず **svuser** のパスワードを定義します。

図 9: svuser のパスワードの初期定義（Windows）

ServerView Operations Manager のアップグレード / 変更インストール中に、svuser のパスワードを変更できます。

図 10: svuser のパスワードの設定（Windows）

次の手順に従って、**svuser** のパスワードを変更します。

1. 「**はい**」を選択し、古いパスワードを入力します。
2. 「**次へ**」をクリックして続行します。

   40 ページ の図 9 に示すダイアログボックスが表示され、**svuser** の新しいパスワードを定義できます。

Linux システムでの svuser のパスワードの変更

ServerView Operations Manager のセットアップ手順中に、まず **svuser** のパスワードを設定します。

コマンド **ChangeComputerDetails.sh** を実行して、いつでもパスワードを変更できます。

ServerView Operations Manager のセットアップの詳細については、『Installing ServerView Operations Manager Software under Linux』マニュアルを参照してください。

3.2.2.3 事前定義されたユーザ Administrator、Monitor、Operator、UserManager の事前定義されたパスワードの変更

> **i** **なお、次の点に注意してください。**
>
> 事前定義されたユーザ **Administrator**、**Monitor**、**Operator**、**UserManager** の事前定義されたパスワードは「admin」です。セキュリティ上の理由から、事前定義されたパスワードを変更することを強く推奨します。

Administrator、**Monitor**、**Operator**、**UserManager** の事前定義されたパスワードは、Operations Manager の開始ウィンドウで「**ユーザ管理**」リンクを選択して変更できます。**UserAdministrator** の役割（またはこれに基づく役割）を持つユーザがクリックすると、**UserManagement** は自動的に「**ユーザ管理**」ウィザードを起動し、1 回のステップですべての事前定義されたパスワードを変更できます。

> **i** CMS での Operations Manager のセットアップが正常に完了した後、**UserManager** が最初に **UserAdministrator** の役割の権限を保有する唯一のユーザになります。このため、**UserManager** が 1 回のステップですべての事前定義されたパスワードを変更することをベストプラクティスとして推奨します。

詳細は 43 ページ の「ApacheDS でのユーザ、役割、権限の管理」の項を参照してください。

3.2.3 ApacheDS でのユーザ、役割、権限の管理

ServerView の「**ユーザ管理**」ウィザードでは、ApacheDS で ServerView ユーザ管理を簡単に実行できます。具体的には、「**ユーザ管理**」ウィザードで次のタスクを実行できます。

– 役割を作成、変更、削除する。

– 権限を役割に割り当てる。

– ユーザを作成、変更、削除する。

– 役割をユーザに割り当てます。

i 「**ユーザ管理**」ウィザードを使用するには、**UserAdministrator** 役割（またはこれに基づく役割）が割り当てられている必要があります。割り当てられていない場合は、自分のパスワードの変更のみが許可されています。

3.2.3.1 ServerView ユーザ管理の開始

ServerView ユーザ管理は、Operations Manager 開始ウィンドウの「**セキュリティ**」にある「**ユーザ管理**」リンクをクリックして開始します。

図 11: ServerView Operations Manager - Start window

i Operations Manager セットアップ中に、JBoss で「組み込み」モードで実行される ApacheDS ではなく、別のディレクトリサービス（Active Directory など）が指定された場合は、「**ユーザ管理**」リンクは表示されません。

UserAdministrator 役割で付与される権限を割り当てられているかどうかに従って、次の事項が適用されます。

– 必要な権限がない場合、自分のパスワードを変更するためのダイアログボックスが開きます（45 ページを参照）。

– **必要な権限がある場合、**「**ユーザ管理**」ウィザードが開始します（46 ページを参照）。

3.2.3.2 ApacheDS のユーザ固有のパスワードの変更

このダイアログボックスで、ApacheDS の自分のパスワードを変更できます。

図 12: Apache DS の自分のパスワードを変更するダイアログボックス

古いパスワードを入力してください。
古いパスワードを入力します。

新しいパスワードを入力してください。
新しいパスワードを入力します。

新しいパスワードを確認してください。
確認のために、新しいパスワードを再入力します。

OK
新しいパスワードが有効になります。

キャンセル
パスワードを変更しないでダイアログボックスを閉じます。

3.2.3.3 「ユーザ管理」ウィザード

「**ユーザ管理**」ウィザードを開始すると、「**ロール定義**」ダイアログボックスが表示されます。

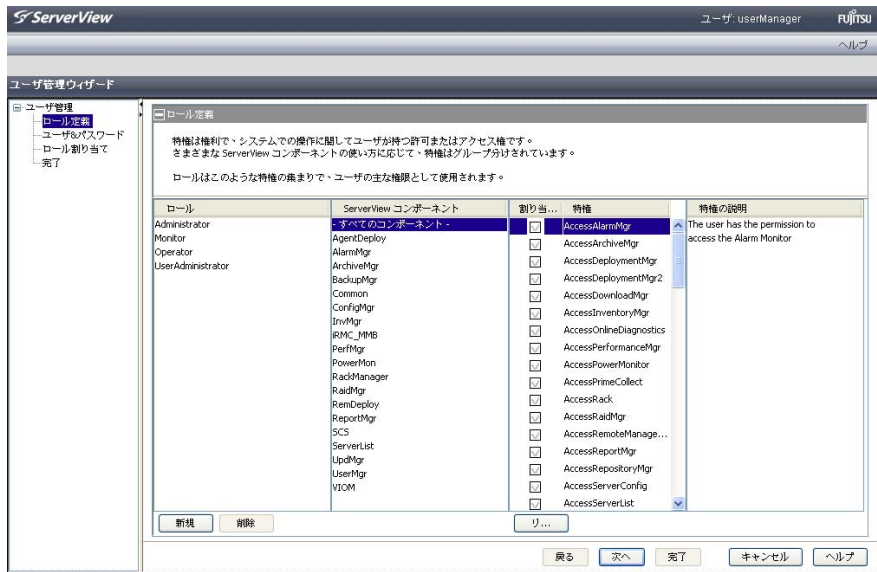



図 13: 「ユーザ管理」ウィザード - 「ロール定義」ダイアログボックス

「**ユーザ管理**」ウィザードには 4 つのステップがあります。ステップが左側のツリー構造に表示されますが、この順序で実行する必要はありません。また、「**ロール定義**」、「**ユーザ & パスワード**」、「**ロール割り当て**」の 3 つのステップをそれぞれ独立して実行することもできます。設定を行ったら、「**完了**」ステップで最終的に設定を反映させてウィザードを終了します。

各ステップで右下のボタンを使用してウィザードを進めることができます。

前へ

ウィザードの前のステップに戻ります。

次へ

ウィザードの次のステップへ進みます。

終了

ウィザードを閉じて、すべての設定を適用します。

「**完了**」ボタンは「**完了**」ステップでのみ有効になります。

キャンセル

変更内容を保存せずにウィザードをキャンセルします。

「**ユーザ管理**」ウィザードのダイアログボックスの詳細については、以下を参照してください。

ロール定義

「**ロール定義**」ダイアログボックスでは、新しい役割の定義、既存の役割の削除、権限と役割の割り当ての有効化と無効化を行えます。ダイアログボックスには、現在定義されているすべての役割と関連する権限が表形式で表示されます。

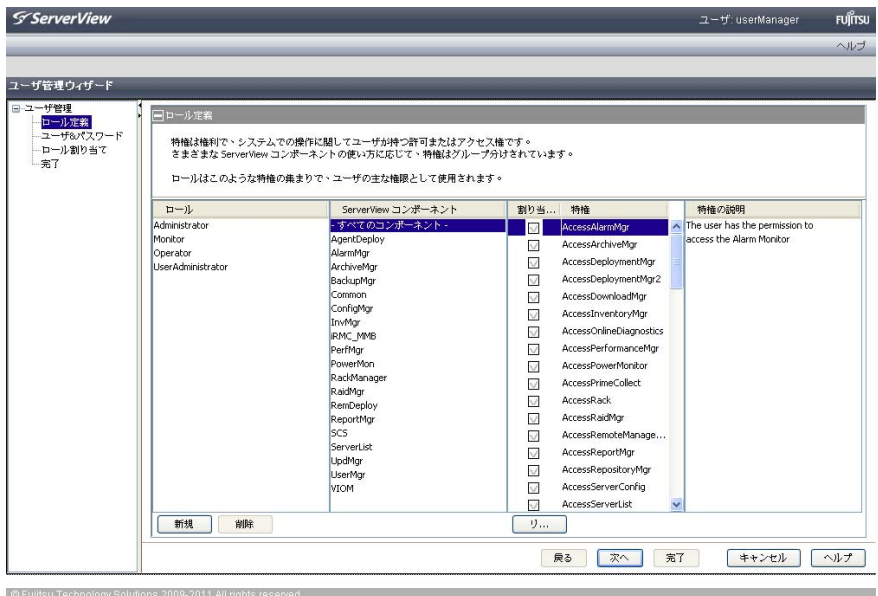



図 14: 「ユーザ管理」ウィザード - 「ロール定義」ダイアログボックス

役割

現在定義されているすべての役割を一覧表示します。事前定義された役割 **Administrator**、**Monitor**、**Operator**、**UserAdministrator** はリストの先頭に表示されます。役割を選択すると、関連する権限が「特権」列に表示されます。

ServerView コンポーネント

使用できるすべての権限カテゴリを一覧表示します。各カテゴリは特定の ServerView コンポーネントの使用または特定のタスクの実行に必要な権限をグループ化したものです。1 つ以上のカテゴリを選択すると、「割り当て特権」に表示される権限を選択したカテゴリに関連するものだけに制限できます。

i 詳細については、110 ページ の「権限カテゴリと関連する権限」の項を参照してください。

割り当て特権

使用できるすべての権限を一覧表示します。1 つ以上の権限カテゴリを「**ServerView コンポーネント**」で選択しているかどうかに応じて、選択したカテゴリで使用できる権限のみが表示されます。対応する「**割り当て済**」オプションを選択または選択解除して、権限と役割の割り当てを有効または無効にすることができます。

i 事前定義された役割 **Administrator**、**Monitor**、**Operator**、**UserAdministrator** の権限割り当ては固定されています。権限と役割の割り当てに対応するオプションは無効になります（グレー表示）。

権限の詳細

選択した権限の簡単な説明を示します。

新規

「**新規**」をクリックすると、「**新しいロール**」ダイアログボックスが開きます。

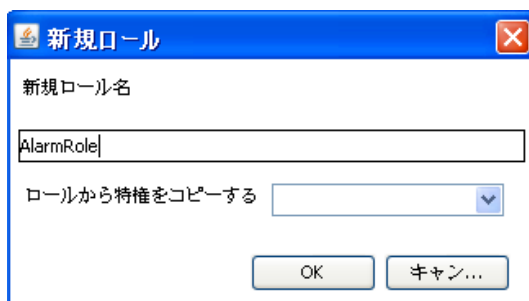



図 15: 「ユーザ管理」ウィザード - 新しいロールの定義

役割名

新しい役割の名前。

ロールから特権をコピーする

ここで、以前定義した役割をリストから選択できます。この場合、選択した役割に割り当てられた権限が、新しい役割に自動的に割り当てられます。

OK

新しい役割を有効にし、「**新しいロール**」ダイアログボックスを閉じます。新しい役割が、「**ロール**」に表示されます。

キャンセル

新しい役割を定義せずに、「**新しいロール**」ダイアログをキャンセルします。

削除

選択した役割を削除します。

リセット

現在表示されている権限と役割の割り当てを、最後に保存された設定にリセットします。

ユーザ & パスワード

「**ユーザ & パスワード**」ダイアログボックスでは、現在 ApacheDS で定義されているユーザ / パスワードのすべての組み合わせを一覧表示し、次の操作を実行できます。

– 新しいユーザを定義する。

– 既存のユーザのパスワードを変更する。

– 既存のユーザを削除する。

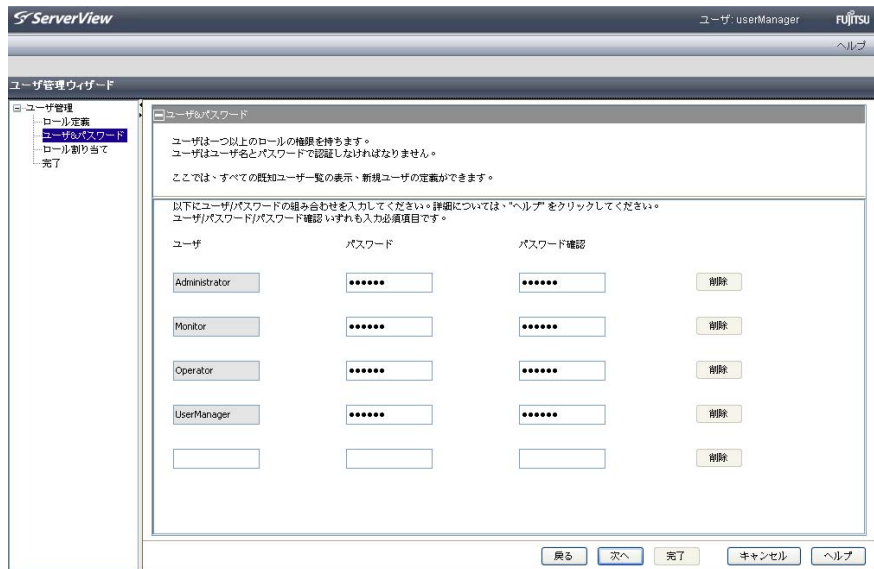



図 16: 「ユーザ管理」ウィザード - 「ユーザ & パスワード」ダイアログボックス

i 4 つの事前定義されたユーザ **Administrator**、**Monitor**、**Operator**、**UserManager** がリストの先頭に表示され、これらは削除できません。ただし、**Administrator**、**Monitor**、**Operator**、**UserManager** のパスワードは変更できます。

リストの末尾には、「**ユーザ**」、「**パスワード**」、「**パスワード確認**」に入力フィールドが空白の未使用の行が表示されており、新しいユーザを定義できます。

User

名前

パスワード

新しいパスワード

確認用パスワード

確認のために、新しいパスワードを再入力します。

削除

関連するユーザを削除します。

リセット

関連するユーザの設定を、最後に保存された設定にリセットします。

ロール割り当て

「ロール割り当て」ダイアログボックスでは、ユーザに役割を割り当てたり、割り当てを解除したりすることができます。ダイアログボックスには、すべての定義されたユーザと役割が表形式で表示されます。現在選択されているユーザに割り当てられている役割にはマークが付けられています。

「ロール割り当て」ダイアログのレイアウトは、ServerView Operations Manager のセットアップ時に統一 RBAC 管理を構成したかどうかによって異なります。

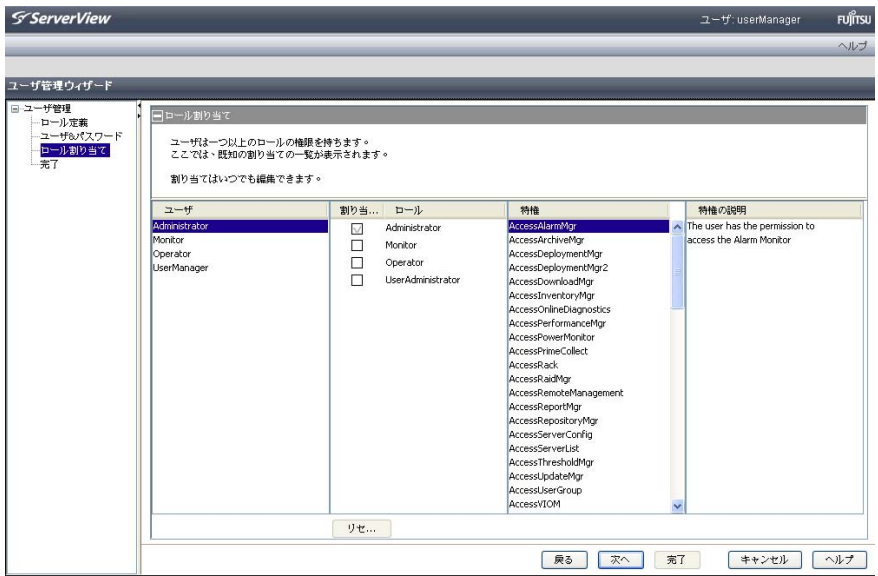



図 17: 「ロール割り当て」ダイアログ（統一 RBAC 管理が無効）

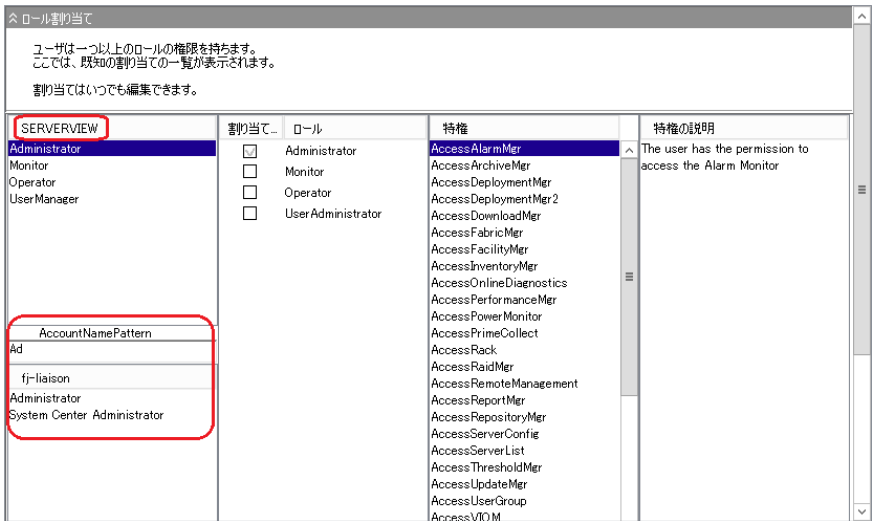



図 18: 「ロール割り当て」ダイアログ（統一 RBAC 管理が有効）

User

統一 RBAC 管理が無効な場合のみ表示されます（『Installing ServerView Operations Manager Software under Windows』マニュアルを参照）。

定義されたすべてのユーザを一覧表示します。ユーザを選択すると、そのユーザに現在割り当てられている役割が「**割り当てロール**」列に表示され、関連する「**割り当て済**」オプションが選択されます。

i 事前に定義されているユーザ **Administrator**、**Monitor**、**Operator**、**UserManager** がリストの先頭に表示されます。これらのユーザへの役割の割り当ては削除できません。

User (SERVERVIEW) および User (< 外部 >)

統一 RBAC 管理が有効な場合のみ表示されます（『Installing ServerView Operations Manager Software under Windows』マニュアルを参照）。

定義されたすべてのユーザを一覧表示します。

– 「**User (SERVERVIEW)**」には、ドメイン SERVERVIEW のすべてのユーザが表示されます。これらのユーザの認証と承認は、どちらも ApacheDS で管理されます。

– 「**User (< 外部ドメイン >)**」には、外部ドメインのすべてのユーザが表示されます。これらのユーザの認証は外部ディレクトリサービス（Active Directory など）で管理され、承認は ApacheDS で管理されます。

ユーザを選択すると、そのユーザに現在割り当てられている役割が「**割り当てロール**」列に表示され、関連する「**割り当て済**」オプションが選択されます。

i 事前に定義されているユーザ **Administrator**、**Monitor**、**Operator**、**UserManager** がリストの先頭に表示されます。これらのユーザへの役割の割り当ては削除できません。

割り当てロール

定義されたすべての役割を一覧表示します。各役割の前には「**割り当て済**」オプションがあり、関連する役割が現在選択されたユーザに割り当てられているか（オプションがオン）、割り当てられていないか（オプションがオフ）が示されます。

対応する「**割り当て済**」オプションをオン / オフして、役割とユーザの割り当てを有効 / 無効にすることができます。

コミュニティの権利

現在選択したユーザに割り当てられている役割に割り当てられた、累積権限を表示します。

権限の詳細

選択した権限の簡単な説明を示します。

リセット

役割とユーザの割り当てを、最後に保存された設定にリセットします。

終了

「**完了**」ダイアログボックスには、現在の「**ユーザ管理**」セッションで実行したステップの概要が表示されます。「**完了**」をクリックすると設定が反映され、ウィザードが閉じられます。

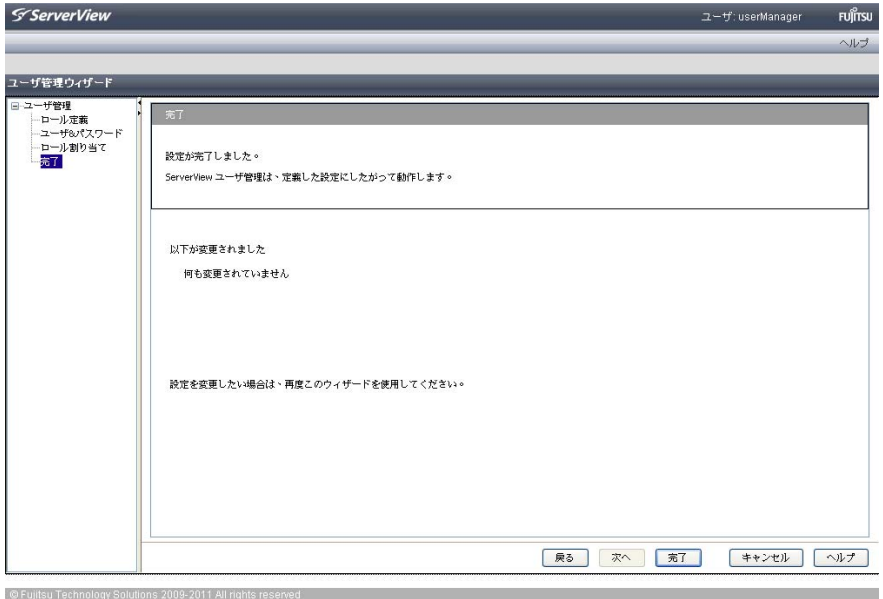



図 19: 「ユーザ管理」ウィザード - 「完了」ダイアログボックス

3.2.4 ApacheDS および SSO を使用する ServerView ユーザ管理への iRMC S2/S3/S4 の統合

iRMC S2/S3/S4 を、ApacheDS を使用する ServerView ユーザ管理に統合し、ServerView Suite SSO ドメインに参加するように設定するには、次の 2 つのステップを実行します。このとき、iRMC S2/S3/S4 Web インターフェースを使用できます。

1. iRMC S2/S3/S4 を、ServerView Operations Manager のセットアップ時にインストールされた ApacheDS ディレクトリサービスを使用するように適切に設定します。

2. iRMC S2/S3/S4 Web インターフェースを、ServerView Suite 内部で CAS ベースのシングルサインオン（SSO）認証用に設定します。

注意事項 :

– CAS サービスを、SSO ドメインに参加しているすべての iRMC S2/S3/S4 に対して設定する必要があります（詳細は、『iRMC S2/S3 - integrated Remote Management』マニュアルおよび『iRMC S4 - integrated Remote Management Controller』マニュアルを参照）。

– 以下では、iRMC S2/S3/S4 を、ApacheDS を使用する ServerView ユーザ管理に統合し、ServerView Suite SSO ドメインに参加するために必要な設定を重点的に説明します。iRMC S2/S3/S4 ディレクトリサービスの設定および iRMC S2/S3/S4 CAS 設定の一般的な情報は、『iRMC S2/S3/S4 - integrated Remote Management Controller』および『iRMC S4 - integrated Remote Management Controller』マニュアルを参照してください。

3.2.4.1 ApacheDS を使用する ServerView ユーザ管理への iRMC S2/S3/S4 の統合

iRMC S2/S3/S4 Web インターフェースの「**ディレクトリサービス構成**」ページでは、ServerView Operations Manager のセットアップ時にインストールされた ApacheDS ディレクトリサービスによるグローバル iRMC S2/S3/S4 ユーザ管理を設定できます。必要な設定を図 20 に示し、以下で説明します。

ディレクトリサービス構成設定

LDAPを有効にする: ☑
LDAP SSL接続を有効にする: ☑
ローカルIDでのログインを無効にする [1]: ☐
常にSSLログインを使用する [2]: ☑
ディレクトリサーバタイプ: OpenDS

プライマリ LDAP Server

LDAPサーバ: my-cms.my-domain
LDAPポート: 1473
LDAP SSLポート: 1474

バックアップ LDAP Server

LDAPサーバ: 0.0.0.0
LDAPポート: 389
LDAP SSLポート: 636

Dept. name: DEFAULT
Base DN: dc=fujitsu,dc=com
Base DN配下のグループディレクトリ:
User Search Context:

適用

注(1): 警告：この設定を行うとディレクトリサーバがアクセス不可能な場合にはログインできません!
注(2): LDAPが無効な場合でもhttpsログインを使用します.

ディレクトリサービスアクセス構成

LDAP 状態: 無効のLDAPサーバ
LDAP認証パスワード: ●●●●●●●●●●●●●●●●●●●●
確認用パスワード:
Principal User DN: CN=svuser,ou=users
Principal User DNに Base DNを追加する: ☑
Bind DN: CN=svuser,ou=users
拡張ユーザ ログイン: ☑
ユーザ ログイン検索フィルタ: (uid=%s)

適用 | LDAP アクセステスト | LDAP状態のリセット

図 20: iRMC S2/S3/S4 の ApacheDS を使用するユーザ管理に対する設定

「ディレクトリサービス構成設定」グループに以下の設定が必要にあります。

1. 「**LDAP を有効にする**」と「**LDAP SSL 接続を有効にする**」を選択します。
2. 「**ディレクトリサーバタイプ**」で、「**OpenDS**」を選択し、「**適用**」をクリックします。
3. 「**プライマリ LDAP Server**」で、次の設定を指定します。
   - **LDAP サーバ** : CMS の DNS 名

     ここでは、Operations Manager を CMS にインストールしたときに指定したものと同じ名前を指定してください。
   - **LDAP ポート** : 1473
   - **LDAP SSL ポート** : 1474
4. 「**Dept. name**」では、デフォルト部署名「`DEFAULT`」を指定します。
5. 「**Base DN**」に「`dc=fujitsu,dc=com`」と入力します。
6. 「**適用**」をクリックして、設定を有効にします。

「ディレクトリサービスアクセス構成」グループで必要な設定「ディレクトリサービスアクセス構成」グループで必要な設定

1. 「**Principal User DN**」に「`cn=svuser,ou=users`」と入力します。
2. 「**Principal User DN に Base DN を追加する**」を選択する
3. 「**拡張ユーザログイン**」を選択し、「**適用**」をクリックします。
4. 「**ユーザログイン検索フィルタ**」に、「`(uid=%s)`」と入力します。
5. 「**LDAP アクセステスト**」をクリックして LDAP 接続のステータスをテストします。この結果は「**LDAP 状態**」に表示されます。
6. 「**適用**」をクリックして、設定を有効にします。

3.2.4.2 iRMC S2/S3/S4 Web インターフェースの CAS ベースのシングルサインオン（SSO）認証用の設定

iRMC S2/S3/S4 Web インターフェースの「**Centralized Authentication Service（CAS）設定**」ページでは、CAS ベースのシングルサインオン（SSO）認証に関連する iRMC S2/S3/S4 の Web インターフェースを設定できます。

必要な設定を図 21 に示します。

図 21: ServerView Suite SSO ドメインに参加させるための iRMC S2/S3/S4 の 設定

以下の設定を行います。

1. **「CAS を有効にする」**を選択します。
2. **「CAS サーバ」**に、CMS の DNS 名を入力します。

   SSO ドメインに参加するすべてのシステムは、必ず同じアドレス表記を使用して中央管理用サーバ（CMS）を参照する必要があります。（「SSO ドメイン」は、同じ CAS サービスを使用して、認証を行うすべてのシステムで構成されます。）そのため、たとえば「my-cms.my-domain」という名前を使用して ServerView Operations Manager をインストールした場合、これとまったく同じ名前を使用して iRMC S2/S3/S4 の CAS サービスを指定します。そうせずに、「my-cms」のみや my-cms の別の IP アドレスを指定しても、SSO は 2 つのシステム間で有効になりません。

3. **「CAS ログイン URL」**と**「CAS ログアウト URL」**で、事前設定された値（**/cas/login**、**/cas/logout**、**/cas/validate**）をそのまま残します。
4. **「SSL 証明書を検証する」**オプションをオンにします。

   セキュリティ上の理由から、SSL 証明書の検証を有効にすることを強く推奨します。**「SSL 証明書を検証する」**オプションをオンにするほかに、SSL 検証を有効にするには、CMS のサーバ証明書を iRMC S2/S3 の認証データ設定にロードしておく必要があります。SSL 証明書を iRMC S2/S3/S4 にアップロードする方法については、『iRMC S2/S3 - integrated Remote Management Controller』および『iRMC S4 - integrated Remote Management Controller』マニュアルを参照してください。

5. **「アクセス許可の割り当て」**で、**「LDAP 経由で割り当てられた許可」**を選択します。
6. **「適用」**をクリックして、設定を有効にします。

3.2.5 ApacheDS データのバックアップとリストア

この節では、以下の操作を実行するために CMS で ApacheDS のコマンド **ldapsearch** および **ldapmodify** を使用する方法について説明します。

– ApacheDS ディレクトリサーバの内部データベースのバックアップを作成する。

– 適用可能なバックアップから ApacheDS ディレクトリサーバの内部データベースをリストアする。

i 使用するバックアップが作成されてからパスワードを変更している場合、パスワードの変更がリストア中に上書きされます。

i OpenLDAP コマンドの **ldapsearch** および **ldapmodify** の包括的な説明については、*www.openldap.org* を参照してください。

3.2.5.1 ApacheDS ディレクトリサーバの内部データベースのバックアップ

ApacheDS の LDAP コンテンツをバックアップするには、OpenLDAP コマンド **ldapsearch** を使用して **exported_data.ldif** ファイルを作成します。

i **exported_data.ldif** ファイルを使用して、ApacheDS の LDAP コンテンツをリストアできます（62 ページ の「ApacheDS ディレクトリサーバの内部データベースのリストア」の項を参照）。

Windows システムでの ApacheDS の LDAP コンテンツのバックアップ

Windows システムでは、次の手順に従います。

1. Windows コマンドプロンプトを開きます。
2. ディレクトリを **<ServerView ディレクトリ >\apacheds\bin** に変更します。
3. 次のコマンドを 1 行で入力して、**exported_data.ldif** ファイルを作成します。

```
ldapsearch -h hostname:1473 -D "cn=Directory Manager" -w
<password> -s sub -b "dc=fujitsu,dc=com" > exported_data.ldif
```

4. 後で使えるように **exported_data.ldif** ファイルを保存します。

Linux システムでの ApacheDS の LDAP コンテンツのバックアップ

Linux システムでは、次の手順に従います。

1. コマンドシェルを開きます。
2. 次のコマンドを 1 行で入力して、**exported_data.ldif** ファイルを作成します。

```
ldapsearch -h hostname:1473 -D "cn=Directory Manager" -w
<password> -s sub -b "dc=fujitsu,dc=com" > exported_data.ldif
```

3. 後で使えるように **exported_data.ldif** ファイルを保存します。

3.2.5.2 ApacheDS ディレクトリサーバの内部データベースのリストア

OpenLDAP コマンド **ldapmodify** を使用して、事前に作成した **exported_data.ldif** ファイルから ApacheDS LDAP コンテンツをリストアできます（61 ページ の「ApacheDS ディレクトリサーバの内部データベースのバックアップ」の項を参照）。

Windows システムでの ApacheDS LDAP コンテンツのリストア

Windows システムでは、次の手順に従います。

1. Windows コマンドプロンプトを開きます。
2. ディレクトリを **<ServerView directory>apacheds\bin** に変更します。
3. 次のコマンドを 1 行で入力して、**exported_data.ldif** ファイルから Apache DS LDAP コンテンツをリストアします。

```
ldapmodify -h hostname:1473 -D "uid=admin,ou=system" -w
<password> -a -c -f exported_data.ldif
```

Linux システムでの ApacheDS LDAP コンテンツのリストア

Linux システムでは、次の手順に従います。

1. コマンドシェルを開きます。
2. 次のコマンドを 1 行で入力して、**exported_data.ldif** ファイルから Apache DS LDAP コンテンツをリストアします。

```
ldapmodify -h hostname:1473 -D "uid=admin,ou=system" -w
<password> -a -c -f exported_data.ldif
```

3.3 ServerView ユーザ管理の Microsoft Active Directory への統合

なお、次の点に注意してください。

ServerView および　iRMC S2/S3/S4 ユーザ管理の設定を行うには、Active Directory に関して熟知している必要があります。ディレクトリサービスを熟知した管理者以外は作業を行わないでください。

Microsoft Active Directory を使用して統合 ServerView ユーザ管理および iRMC S2/S3/S4 ユーザ管理を操作する前に、以下の予備手順に従います。

1. ServerView Suite の役割定義（Administrator、Operator、Monitor 36 ページを参照）を Active Directory にインポートします。
2. iRMC S2/S3/S4 役割定義を Active Directory にインポートします。
3. 役割をユーザに割り当てます。
4. Active Directory サーバへのセキュアな LDAP（LDAPS）アクセスを設定します。

手順については、以下で詳しく説明します。

注意事項 :

– 統一 RBAC 管理を ServerView Operations Manager に対して構成する場合は、ステップ 1 ～ 3 は必要ありません。

  この場合、ServerView Operations Manager の「内部」ディレクトリサービス（ApacheDS）が、ユーザへの役割の割り当てに常に使用されます。Active Directory は、ユーザ承認を目的としてのみアクセスされます。統一 RBAC 管理の詳細については、25 ページ の「既存の設定済みディレクトリサービスと RBAC との連携」の項 および『Installation of ServerView Operations Manager Software on Windows / Linux』マニュアルを参照してください。

– 認証設定が iRMC S4 にある標準 LDAP グループを iRMC S4 に対して構成する場合は、ステップ 2 と 3 は必要ありません。

  認証設定が iRMC S4 にある標準 LDAP グループを iRMC S4 Web インターフェースで構成し、これを使用して Active Directory の標準 LDAP グループに属するユーザに iRMC S4 権限と許可定義することができます。詳細は、マニュアル『iRMC S4 - integrated Remote Management Controller』を参照。

前提条件：

ステップ 2 と 3 で、ServerView ユーザ管理と iRMC S2/S3/S4 ユーザ管理を Active Directory に統合するには、次のファイルが必要です。

- **ServerView ユーザ管理の場合：**

  Active Directory での統合には、ServerView 固有の構造を含む LDIF（Lightweight Directory Interchange Format）ファイル。

  Operations Manager のインストール時に、使用するディレクトリサービスとして Active Directory を選択した場合、Operations Manager がインストールされている CMS の以下のディレクトリで必要な LDIF ファイルを見つけます。

  – Windows システムの場合：
    <ServerView ディレクトリ>￥svcommon￥files￥SVActiveDirectory.ldif

  – Linux システムの場合：
    /opt/fujitsu/ServerViewSuite/svcommon/files/SVActiveDirectory.ldif

- **iRMC S2/S3/S4 ユーザ管理の場合：**

  XML 構文による Active Directory での **SVS** 構造のストラクチャ情報を含む **XML** 設定ファイル。「**SVS_LdapDeployer**」（144 ページを参照）はこの **XML** 設定ファイルに基づいて LDAP ストラクチャを生成します。設定ファイルの構文については、サンプル設定ファイル「**Generic_Settings.xml**」および「**Generic_InitialDeploy.xml**」で説明されています。これらのファイルは、ServerView Suite DVD に収録される **jar** アーカイブ「**SVS_LdapDeployer.jar**」の中にあります。

注意事項：

ServerView ユーザ管理と iRMC S2/S3/S4 グローバルユーザ管理の両方を同じ組織単位（OU）**SVS** で動作させるには、iRMC S2/S3/S4 ユーザ管理が **DEFAULT** 部門に属するように設定する必要があります。

次の手順に従います。

1. **ServerView のユーザ役割定義をインポートします。**

   a) Active Directory を実行している Windows システムの一時ディレクトリに **SVActiveDirectory.ldif** ファイルをコピーします。

   b) Windows コマンドプロンプトを開き、**SVActiveDirectory.ldif** ファイルを含むディレクトリに移動します。

   c) Microsoft の **ldifde** ツールを使用して LDIF ファイルをインポートします。

```
ldifde -i -e -k -f SVActiveDirectory.ldif
```

i **ldifde** ツールがシステムの **PATH 変数**に含まれていない場合は、**%WINDIR%¥system32** ディレクトリにあります。

i 必要に応じて、既存の LDAP 構造を新しい権限に追加します。ただし、既存のエントリが影響を受けることはありません。

これで、追加した権限および役割が Active Directory GUI に表示されます（65 ページ の図 22 を参照）。

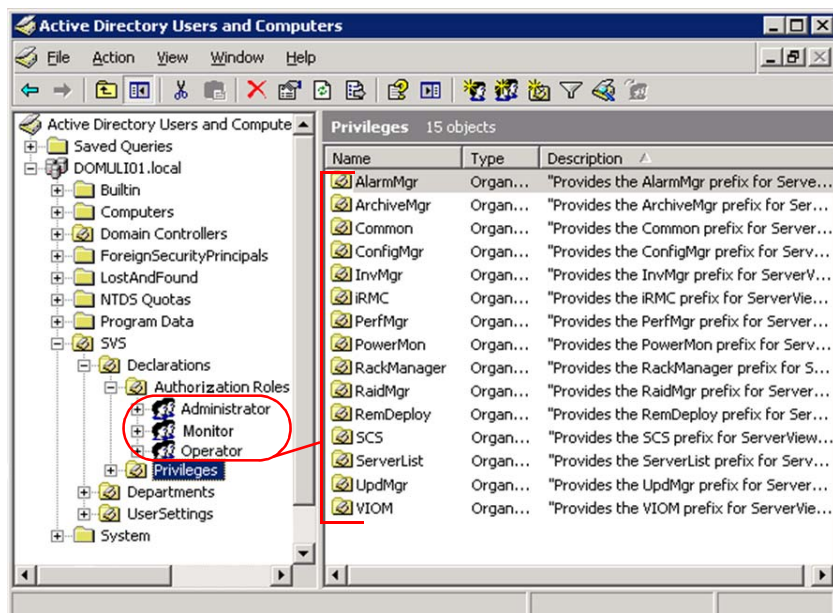



図 22: Active Directory GUI に表示される追加した権限およびユーザ役割

2. **iRMC S2/S3/S4 ユーザ定義をインポートします。**

   ソフトウェアツール **SVS_LdapDeployer** を使用して iRMC S2/S3/S4 ユーザ役割定義を Active Directory にインポートします。詳細は 152 ページ の「SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除」の項を参照してください。

3. **ユーザ役割をユーザとグループに割り当てます。**

   i 以下で説明する手順では、例として、**Monitor** 役割を、Active Directory ドメイン「DOMULI01」でのユーザログイン名が「NYBak」の、「John Baker」に割り当てると想定します。

   i 以下で説明するステップは、iRMC S2/S3/S4 ユーザへの役割の割り当てにも適用されます。iRMC S2/S3/S4 ユーザへの役割の割り当てについては、166 ページ の「iRMC S2/S3 ユーザへのユーザロールの割り当て」の項および 247 ページ の「iRMC S4 ユーザへのユーザロールの割り当て」の項を参照してください。

   i 役割が割り当てられるユーザーのアカウント情報を含む LDAP オブジェクトが、必ず設定されたユーザ検索ベースの下に配置されるようにしてください。（ユーザ検索ベースは、ServerView Operations Manager のセットアップ時に設定されます。詳細については、対応するインストールマニュアルを参照してください。）

   i 同様に、役割をグループに割り当てる場合は、グループのすべてのメンバの LDPA オブジェクトが、必ず設定されたユーザ検索ベースの下に配置されるようにしてください。

   a) CMS で **「スタート」- 「コントロールパネル」- 「管理ツール」- 「Active Directory ユーザとコンピュータ」**を選択し、Active Directory GUI を起動します。

b) GUI のツリー構造で、**SVS** ノードから **Departments** ノードに移動します。「Departments」の **CMS** および **DEFAULT** を展開します（図 23 を参照）。

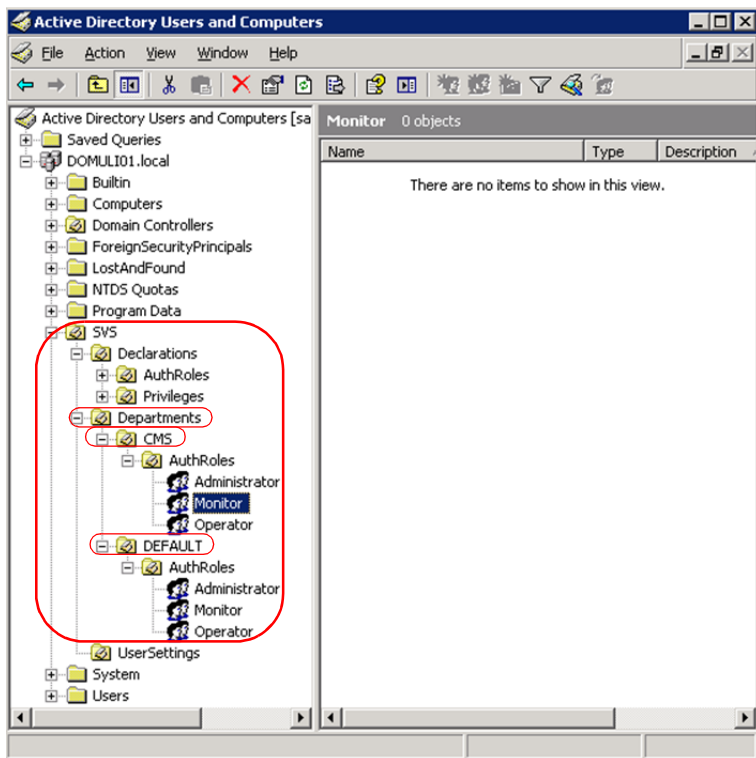



図 23: Monitor 役割をユーザ（John Baker）に割り当てます。

c) **「SVS」-「Departments」-「CMS」-「AuthRoles」**で、**「Monitor 」**を右クリックし、**「プロパティ」**を選択します。

「Monitor」役割の**「プロパティ」**ダイアログが表示されます。

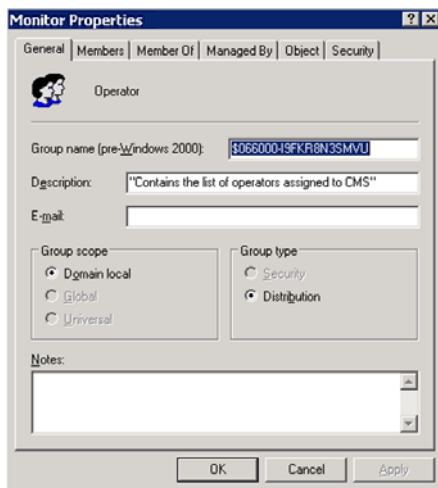



図 24: 「Monitor」役割の「プロパティ」ダイアログボックス

d) **「メンバー」**タブを選択し、**「追加 ...」**をクリックします。

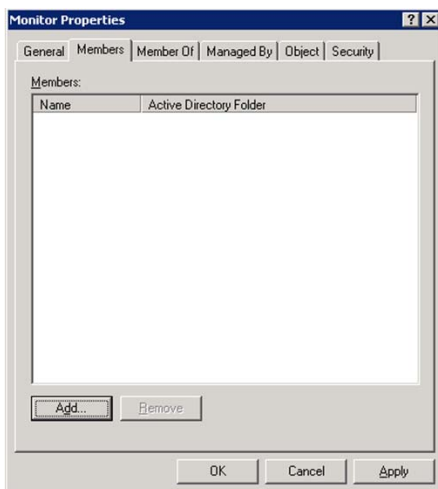



図 25: Monitor の「プロパティ」ダイアログ - 「メンバー」タブ

「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログが表示されます。

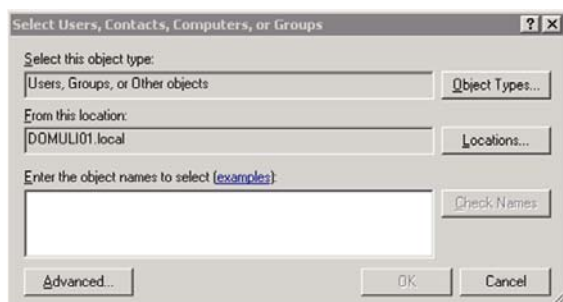



図 26: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ

e) **「詳細設定」**をクリックしますと共に提供されます。

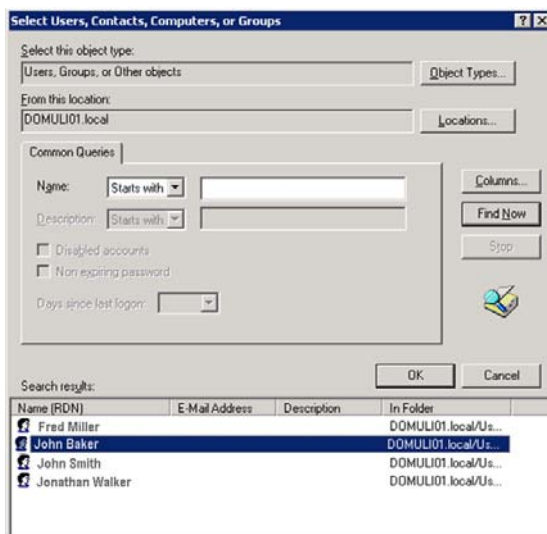



図 27: 必要なユーザを選択します。

「検索結果」リストで**「ログイン名」**列を選択してから、**「今すぐ検索」**をクリックすると、**「名前」**を制限して検索を迅速に行うことができます。

f) 必要なユーザまたはグループを選択し、「**OK**」をクリックします。

これで、ユーザ「Baker」が上位ダイアログの「**オブジェクト名**」リストに表示されます。

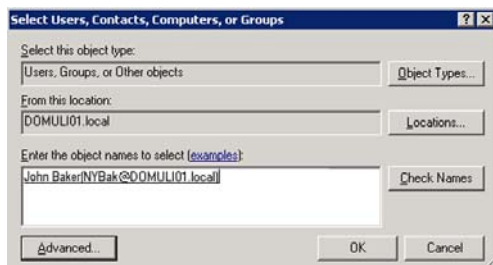



図 28: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ : ユーザ「Baker」の表示

g) 「**OK**」をクリックします。

これで、ユーザ「Baker」が「**Monitor のプロパティ**」ダイアログの「**メンバー**」タブに表示されます。

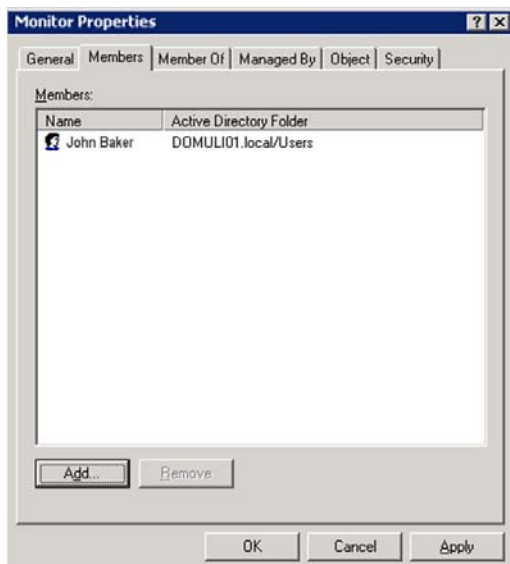



図 29: Monitor の「プロパティ」ダイアログ - 「メンバー」タブ : ユーザ「Baker」の表示

h)　**c ～ g** の手順を「Department」の **DEFAULT** に繰り返します。

4. Active Directory サーバへのセキュアな LDAP（LDAPS）アクセスを設定します。

   Operations Manager のインストール手順では、ユーザ管理を行うディレクトリ サーバへの LDAP アクセスを設定する必要があります。Active Directory では、デフォルトではポート 389 でセキュアでない LDAP インターフェースを提供しています。このインターフェースはテスト目的にご利用いただけます。

   ただし、実稼働環境を設定する場合は、Active Directory サーバに安全な LDAPS インターフェースを確立してください。この場合、このサーバにサーバ証明書をインストールする必要があります。

   i 詳細は、Microsoft（*http://support.microsoft.com*）関連のマニュアル『*How to enable LDAP over SSL with a third-party certification authority*』を参照してください。

   iRMC S2/S3/S4 LDAP/SSL アクセスの設定については、161 ページ の「Active Directory サーバ上の iRMC S2/S3 LDAP/SSL アクセスの設定」の項または242 ページ の「Active Directory サーバ上の iRMC S4 LDAP/SSL アクセスを設定します。」の項を参照してください。

   テストの場合は、Active Directory サーバに自己署名証明書をインストールすれば十分です。これは、IIS 6.0 Resource Kit Tools の **selfssl.exe** ツール（*http://support.microsoft.com* からダウンロード可能）を使用して容易に行うことができます。

   例：

   キーの長さが 2048 ビットで 2 年間有効な自己署名証明書をサーバ **myserver.mydomain** にインストールするには、次の手順に従います。

   ► Windows コマンドプロンプトを開いて以下のコマンドを入力します。

   ```
   selfssl /T /N:CN=myserver.mydomain /K:2048 /V:730
   ```

   selfssl.exe により、以下のメッセージが表示されます。

   ```
   Microsoft (R) SelfSSL Version 1.0Copyright (C) 2003
   Microsoft Corporation.All rights reserved.Do you want to
   replace the SSL settings for site 1 (Y/N)?
   ```

▶ 「Y」と入力します。

次に表示されるメッセージ「Failed to build the subject name blob: 0x80092023」は、IIS がインストールされていないことを指摘しているだけなので無視できます。

ただし、**ldaps: //myserver.mydomain** 経由でアクセスしている場合、Active Directory はインストールされているこの証明書を使用します。

これで、ユーザ「John Baker」は、ユーザ名 NYBak で Operations Manager にログインできます。Baker は、**Monitor** 役割の権限によって許可されたすべての機能を実行できます。

3.3.1 LDAP バインドアカウントのパスワードの変更

40 ページ の「svuser のパスワードの定義 / 変更」の項で記載されている説明と同じ方法で、Active Directory などの「外部」ディレクトリサービスへのアクセスに使用する LDAP バインドアカウントのパスワードを変更できます。

または、バッチスクリプト **SetDSPassword** を使用できます。このスクリプトの使用には、JBoss を再起動しなくてもよいという利点があります。ただし、設定変更が有効になるまで 5 分かかるという点に注意してください。このため、パスワードを変更してからもう一度サインインするまで、必ず 5 分待機してください。

SetDSPassword は Windows または Linux 環境で呼び出せます。

Windows

▶ Windows コマンドプロンプトを開きます。

▶ **<ServerView ディレクトリ >\jboss\standalone\bin** ディレクトリに移動します。

▶ **SetDSPassword <new password>** と入力します。

i
- パスワードには、空白（ ）および二重引用符（"）など、あらゆる印刷可能文字を使用できます。
- パスワードに空白（ ）、二重引用符（"）、コンマ（,）、キャレット（^）、またはその他の特殊文字が使用されている場合、パスワードを二重引用符で囲んでください（例 : "Pa\\w^rd"）。
- バックスラッシュ（\）は、直後に二重引用符がなければ、そのままの形式で解釈されます。

– 直前にバックスラッシュがある二重引用符（\"）は、リテラルとしての二重引用符（"）として解釈されます。

– キャレット（^）は、パスワードが二重引用符で囲まれている場合は、エスケープ文字または区切り文字としては認識されません。

Linux

► xterm ターミナルや gnome ターミナルなどの、ターミナルを開きます。

► **/opt/fujitsu/ServerViewSuite/jboss/standalone/bin** ディレクトリに移動します。

► **./SetDSPassword <new password>** と入力します。

i

– パスワードには、空白（ ）および二重引用符（"）など、あらゆる印刷可能文字を使用できます。

– パスワードに空白（ ）、二重引用符（"）、コンマ（,）、キャレット（^）、またはその他の特殊文字が使用されている場合、パスワードを二重引用符で囲んでください（例 : "Pa\\w^rd"）。

– バックスラッシュ（\）は、直後に二重引用符がなければ、そのままの形式で解釈されます。

– 直前にバックスラッシュがある二重引用符（\"）は、リテラルとしての二重引用符（"）として解釈されます。

– キャレット（^）は、パスワードが二重引用符で囲まれている場合は、エスケープ文字または区切り文字としては認識されません。

3.3.2 LDAP パスワードポリシー適用（LPPE）

ユーザが CAS に認証しようとするとき、以下のようないくつかの特殊な場合（例外）が発生することがあります。

– 現在ログオンできない

– パスワードが期限切れ、またはリセットする必要がある

– ユーザアカウントが無効 / 期限切れ / ロックされている

LPPE がなければ、通常の CAS ログインフローでは上記のシナリオはエラーとみなされ、認証は行われません。LPPE は以下の手順を実行して、標準 CAS ログインを強化します。

1. LPPE は、LDAP 応答ペイロードの一部として返されたエラーコードを検出して、標準認証フローをインターセプトします。

2. LPPE はエラーコードをより正確なエラーメッセージに変換し、CAS ログインフロー内でこのエラーメッセージを表示します。

これにより、ユーザは適切なアクションを実行できます。

現在 LPPE で処理されるログイン例外を 表 3 に示します。

LDAP エラーコード	**LDAP エラーテキスト**	**CAS から表示されるメッセージ**
530	現在ログオンできない	認証時に、ユーザは現在サインオンできないというメッセージを表示します。 **現在ログインする権限がありません。** **アクセスするためにはシステム管理者に問い合わせてください。**
531	このワークステーションにログオンできない	認証時に、アカウントが無効で、ユーザは管理者に連絡する必要があるというメッセージを表示します。 **このワークステーションからログインする権限がありません。** **アクセスするためにはシステム管理者に問い合わせてください。**

表 3: LDAP エラーコード

LDAP エラーコード	LDAP エラーテキスト	CAS から表示されるメッセージ
532	パスワードが期限切れ	認証時に、アカウントのパスワードが期限切れで、セルフサービスパスワード管理アプリケーションへのリンクをオプションで提供するというメッセージを表示します。 **パスワードの有効期限が切れています。 パスワードを変更してください。**
533	アカウントが無効	認証時に、アカウントが無効で、ユーザは管理者に連絡する必要があるというメッセージを表示します。 **このアカウントは無効です。 アクセスするためにはシステム管理者に問い合わせてください。**
701	アカウントが期限切れ	認証時に、アカウントが期限切れだというメッセージを表示します。 **アカウントの有効期限が切れています。**
773	ユーザはパスワードをリセットする必要がある	認証時に、アカウントのパスワードを変更する必要があり、セルフサービスパスワード管理アプリケーションへのリンクをオプションで提供するというメッセージを表示します。 **パスワードを変更する必要があります。 パスワードを変更してください。**
775	ユーザのアカウントがロックされている	認証時に、アカウントが無効で、ユーザは管理者に連絡する必要があるというメッセージを表示します。 **このアカウントは無効です。 アクセスするためにはシステム管理者に問い合わせてください。**

表 3: LDAP エラーコード

パスワードの有効期限

LPPE はユーザパスワードの予期される有効期限も検出します。パスワードの有効期限が近付くと、設定された警告期間内にメッセージが表示されます。認証時に、CAS はユーザのパスワードの期限がまもなく切れるいうメッセージを表示します。

パスワードは本日で有効期限が切れます。パスワードを変更してください。

または

パスワードは明日で有効期限が切れます。パスワードを変更してください。

または

パスワードはあと ... 日で有効期限が切れます。
パスワードを変更してください。

予期されるパスワードの有効期限を検出するため、CAS は一部の LDAP 属性を設定された Active Directory サービスから読み取ります。このためには、以下の設定値が必要です。

ドメイン DN

これは、Active Directory ドメインの**識別名**です。

例

`dc=fujitsu、dc=com`

有効日数

このプロパティの値は、パスワードが有効な日数を示します。これは、**maxPwdAge** 属性が Active Directory にない場合のデフォルト値を定義することに注意してください。つまり、Active Directory で設定された値は常に、ここで設定された値を上書きするということです。

例

`90`

警告日数

このプロパティの値は、ユーザが警告される、パスワードが期限切れになるまでの日数を示します。Active Directory にはこれに対応する属性はありません。したがって、この値はパスワードの期限切れを警告する期間を定義する唯一の値になります。

例

`30`

パスワード変更 URL(任意)

このエントリは、パスワードを変更するためにユーザがリダイレクトされる URL を指定します。この URL のランディングページはユーザに提供する必要があります。ServerView はこのような Web ページを提供しません。ユーザの環境にこのようなページがない場合に、設定オプションを省略してください。

このエントリーはオプションです。通常に Active Directory サービスのユーザ管理にパスワードが変更されます。

例

```
https://www.example.corp.com/UserMgt
```

4 CMS および管理対象ノードでの SSL 証明書の管理

Web ブラウザおよび管理対象ノードと通信するために、CMS ではセキュアな SSL 接続で公開鍵インフラストラクチャ（PKI）を使用します。

この章では、以下のトピックについて説明します。

– 80 ページ の「SSL 証明書の管理（概要）」

– 83 ページ の「CMS での SSL 証明書の管理」

– 95 ページ の「RBAC およびクライアント認証用の管理対象ノードの準備」

「BEAST」および「POODLE」の攻撃を回避するために、JBoss Web サーバは次の SSL/TLS プロトコルのみサポートします。

– ServerView Operations Manager V7.10 では、SSLv2Hello、TLSv1.1、および TLSv1.2 のみサポートします。

– ServerView Operations Manager < V7.10 では、デフォルトで SSLv2Hello、TLSv1.0、TLSv1.1 および TLSv1.2 をサポートします。

  それでも SSLv3 を有効にする場合は、追加の <ssl> タグ（`ds-cfg-ssl-protocol:SSLv3`）を設定ファイル **jboss\standalone\configuration\standalone.xml.orig** に挿入します。

```
ds-cfg-ssl-protocol: TLSv1
ds-cfg-ssl-protocol: SSLv2Hello
ds-cfg-ssl-protocol: SSLv3
```

4.1 SSL 証明書の管理（概要）

Web ブラウザおよび管理対象ノードと通信するために、CMS ではセキュアな SSL 接続で公開鍵インフラストラクチャ（PKI）を使用します。

CMS が自身をサーバ認証により Web サーバで認証する

Web ブラウザは通常、HTTPS 接続（セキュアな SSL 接続）を使用して中央管理用サーバ（CMS）と通信します。そのため、CMS の JBoss Web サーバには、サーバ認証により自身を Web ブラウザに認証するために証明書（X.509 証明書）が必要です。X.509 証明書には、JBoss Web サーバを識別するために必要なすべての情報と、JBoss Web サーバの公開鍵が含まれています。

詳細は、83 ページ の「CMS での SSL 証明書の管理」の項を参照してください。

CMS が自身をクライアント認証により管理対象ノードで認証する

RBAC 機能を使用する管理対象ノード（PRIMERGY サーバなど）には、X.509 証明書ベースのクライアント認証が必要です。そのため CMS は、管理対象ノードに接続するときに、自身を認証する必要があります。クライアント認証により、管理対象ノードが、信頼されない CMS または CMS で実行中の権限のないアプリケーションからアクセスされることを防ぎます。

クライアント認証は、信頼される CMS の証明書があらかじめ管理対象ノードにインストールされていることを前提とします。

詳細は、95 ページ の「RBAC およびクライアント認証用の管理対象ノードの準備」の項を参照してください。

SSL 公開鍵およびセキュリティインタセプタコンフィグレーションファイル

以下のファイルが Operations Manager セットアップ時に自動的に生成されます。

- **< システム名 >.scs.pem**

  PEM 形式の自己署名証明書。PEM ファイルにも公開鍵が含まれます。

  CMS は、以下の目的に **< システム名 >.scs.pem** ファイルを使用します。

  – CMS に接続する Web ブラウザへのサーバ認証。

  – RBAC 機能を使用する管理対象ノードへのクライアント認証。クライアント認証を行うには、**< システム名 >.scs.pem** ファイルを管理対象ノードにインストールする必要があります。

- **< システム名 >.scs.xml**

  セキュリティインタセプタのコンフィグレーションファイルこのファイルは、RBAC 検証呼び出しのために内部で使用されます。管理対象ノードで RBAC 機能を有効にするには、**< システム名 >.scs.xml** ファイルを管理対象ノードにインストールする必要があります。

Operations Manager セットアップで CMS の次のディレクトリに両方のファイルがインストールされます。

– **<ServerView directory>\svcommon\data\download\pki**（Windows システムの場合）

– **/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki**（Linux システムの場合）

i 以降、**< システム名 >.scs.pem** および **< システム名 >.scs.xml** は証明書ファイルと略記します。

鍵ペア（keystore ファイルおよび truststore ファイル）の管理

JBoss Web サーバの Java ベースの鍵と証明書の管理では、2 つのファイルを使用して鍵ペアと証明書を管理します。

– keystore ファイル（ファイル名 :**keystore**）に、JBoss Web サーバは固有の鍵ペアと証明書を保存します。

– truststore ファイル（ファイル名 :**cacerts**）には、JBoss Web サーバが信頼できると評価したすべての証明書が含まれています。

keystore と truststore ファイルは、以下のディレクトリにあります。

– **<ServerView ディレクトリ >\jboss\standalone\svconf\pki**（Windows システムの場合）

– **/opt/fujitsu/ServerViewSuite/jboss/standalone/svconf/pki** （Linux システムの場合）

i **keytool** ユーティリティを使用して keystore ファイルと truststore ファイルを処理します（85 ページを参照）。

4.2 CMS での SSL 証明書の管理

Web ブラウザは、JBoss Web サーバとの通信に常に HTTPS 接続（つまり、セキュア SSL 接続）を使用します。そのため JBoss Web サーバには、自身を Web ブラウザで認証するために証明書（X.509 証明書）が必要です。
X.509 証明書には、JBoss Web サーバを識別するために必要なすべての情報と、JBoss Web サーバの公開鍵が含まれています。

4.2.1 自己署名証明書はセットアップ時に自動的に作成される

PEM 形式の自己署名証明書 (**<system_name>.scs.pem**) は、Operations Manager セットアップ時に（ローカル）JBoss Web サーバに自動的に作成されます。

セットアップで **< システム名 >.scs.pem** が次のディレクトリにインストールされます。

– **<ServerView ディレクトリ >￥svcommon￥data￥download￥pki**（Windows システムの場合）

– **/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki**（Linux システムの場合）

i 自己署名証明書を使用する場合に、ユーザが弊社固有の認証局（CA）の設定や、外部 CA への証明書署名要求（CSR : Certificate Signing Request）の発行に関与することはありません。

ServerView Operations Manger のアップデートインストールが必要な場合（CMS の名前が変更された後など）、自己署名証明書 はアップデートインストール中に自動的に置換されます。

i JBoss Web サーバが自己署名証明書を使用する場合 :
JBoss Web サーバに接続すると、Web ブラウザが証明書エラーを発行し、処理手順を指示します。

可用性が明確なため、自己署名証明書はテスト環境に最適です。ただし、Operations Manager を使用する運用サーバ管理に典型的な高レベルの安全要件を満たすには、信頼される認証局によって署名された証明書（CA 証明書）を使用することを推奨します。

4.2.2 CA 証明書の作成

証明書は、証明書に指定された組織の身元が確認された時点で、中央の認証元である認証局（CA）の秘密鍵を使用して証明書に署名することにより、CA によって発行されます。署名は証明書に含まれ、クライアントが証明書の信頼性を確認できるように、接続セットアップ時に公開されます。

> **なお、次の点に注意してください。**
>
> ServerView Operations Manger のアップデートインストールが必要な場合（CMS の名前が変更された後など）、CA 証明書 はアップデートインストール中に自動的に**置換されません**。代わりに、自分で証明書を置換する必要があります（86 ページ の「中央管理用サーバ（CMS）での証明書の交換」の項を参照）。

CA 証明書を作成するには次の手順を行う必要があります。

1. 証明書署名要求を作成します（CSR。ここでは **certrq.pem**。**openssl** ツールなどを使用します）。

   ```
   openssl req -new -keyout privkey.pem -out certreq.pem
   -days 365
   ```

2. CSR を CA に送信します。

   CA が PEM 形式（**certreply.pem** など）または DER 形式（**certreply.cer** など）の署名された証明書（証明書応答）を返します。

   以下では、証明書は PEM 形式であると仮定します。必要に応じて、以下のコマンドを使用して証明書を DER 形式から PEM 形式に変換できます。

   ```
   openssl x509 -in certreply.cer -inform DER -out
   certreply.pem -outform PEM
   ```

   > 証明書に拡張鍵用途が指定される場合、サーバ証明書とクライアント証明書の両方として使用されるため、鍵用途サーバ認証（1.3.6.1.5.5.7.3.1）およびクライアント認証（1.3.6.1.5.5.7.3.2）に対して署名されていることが重要です。

3. 署名された証明書をファイルに保存します。

4. 署名された証明書を確認します。

4.2.3 証明書と鍵を管理するためのソフトウェアツール

証明書および関連する鍵を管理するには、以下のソフトウェアツールが必要です。

– **openssl**

openssl ツールは、Shining Light Productions の Web サイト（*http://www.slproweb.com*）などからインターネット経由でダウンロードできます。この代わりに、Cygwin 環境（*http://www.cygwin.com*）のインストールも推奨します。

i Shining Light Productions の Web サイトから **openssl** ツールを使用している場合、環境変数 **OPENSSL_CONF** を以下の値に設定する必要があります。

< path to the OpenSSL installation directory>/bin/openssl.cfg

– **keytool**

keytool は Oracle ホームページからダウンロードできます。**keytool** は Java 仮想マシンとは別にインストールされるため、ユーティリティはデフォルトで中央管理用サーバに保存されます。

– Windows システム : **C:￥Program Files (x86)￥Java￥jre7￥bin** など

– Linux システムの場合 : **/usr/java/default/bin**

4.2.4 中央管理用サーバ（CMS）での証明書の交換

この項では、別の証明書に交換する場合に必要な手順について説明します。

前提条件 :

下記の手順を行うには、以下のことが必要です。

– 必要なソフトウェア : **openssl**、**keytool**（85 ページを参照）。

また、次の説明では、**keytool** を含むディレクトリが **PATH** 変数の一部であることを前提とします。

– 署名された CA 証明書（ここでは **certreply.pem**）と秘密鍵（ここでは **privkey.pem**）を用意する必要があります。

中央管理用サーバで証明書を交換した後、管理対象ノードで証明書を交換する必要があります（Windows 管理対象ノードの場合は 100 ページ、Linux/VMware 管理対象ノードの場合は 101 ページを参照）。これにより、CMS は管理対象ノードでの認証を継続できます。

4.2.4.1 Windows システムでの証明書の交換

次の手順に従います。

1. JBoss サービスを停止します（18 ページを参照）。
2. **keystore** ファイルを削除します。
   a) Windows コマンドプロンプトを開きます。
   b) **<ServerView ディレクトリ >\jboss\standalone\svconf\pki** ディレクトリに移動します。
   c) **keystore** ファイルを削除するかファイル名を変更します。
3. CA が署名した証明書応答（ここでは **certreply.pem**）と CA 独自の証明書（ここでは **certca.pem**）を、現在のディレクトリ（**<ServerView ディレクトリ >\jboss\standalone\svconf\pki**）にコピーします。
4. 証明書応答と CA 独自の証明書を新しい **keystore** ファイルにインポートして、公開鍵（ここでは **keystore.p12**）をエクスポートします。

```
openssl pkcs12 -export -chain -in certreply.pem -inkey
privkey.pem -passout pass:changeit -out keystore.p12
-name svs_cms -CAfile certca.pem -caname "%CANAME%"
```

i プレースホルダ %CANAME% を、証明書署名要求に署名した CA の名前に置き換えます。

5. **keystore** ファイルを（再）フォーマットします。

```
keytool -importkeystore -srckeystore keystore.p12
    -destkeystore keystore -srcstoretype PKCS12
    -srcstorepass changeit -deststorepass changeit
    -destkeypass changeit -srcalias svs_cms
    -destalias svs_cms -noprompt -v
```

6. 新しい証明書を **truststore** ファイルにインポートします。

   これを最も容易に行うには以下の手順に従います。
   a) JBoss サービスを開始します。
   b) スタートアップが完了するまで待ちます。
   c) **<ServerView ディレクトリ >\jboss\standalone\bin** ディレクトリに移動します。

d) Windows コマンドプロンプトを開いて以下のコマンドを入力します。

```
java -jar install-cert-gui-SVCOM_V1.70.jar
..\svconf\pki\cacerts changeit <system FQDN>:3170
```

i 設定済みの外部ディレクトリサービス（Active Directory など）を使用する場合は、次のコマンドも入力する必要があります。

```
java -jar install-cert-gui-SVCOM_V1.70.jar
..\svconf\pki\cacerts changeit <system FQDN>:<port>
```

< システム FQDN>
: 各外部ディレクトリサービスシステムの完全修飾識別名です。

<port>
: 外部ディレクトリサービスに使用される LDAP ポート（通常：636）

e) Java プログラム **install-cert-gui-SVCOM_V1.70.jar** により、次のようなパネルが表示されます。

図 30: Add Security Exception

このパネルを使用して、truststore にインポートする認証パス（Certificate Chain）から証明書を選択できます。エントリが 1 つしかない場合、証明書は自己署名式なので、これをインポートする以外に選択肢はありません。そうでない場合、上記例のように証明書が少なくとも 2 つになります。

1. サーバ証明書
2. サーバ証明書に署名した認証局（Certificate Authority : CA）の証明書

一般には、CA 証明書のみのインポートが推奨されます。その結果、同じ CA に署名されたサーバ証明書が自動的に信頼され、多くの場合有効です。

> **i** Java プログラムを呼び出すと、次のメッセージが表示されます
>
> ```
> testConnection(tm,pontresina.servware.abg.firm.net,
> 3170): SSLException: java.lang.RuntimeException:
> Unexpected error:
> java.security.InvalidAlgorithmParameterException: the
> trustAnchors parameter must be non-emptywriting to
> truststore ..\svconf\pki\cacerts...
> ```
>
> これはエラーではなく、新しい証明書がまだ **truststore** ファイルにインポートされていないことを示しているだけです。

f) PEM 形式の **keystore.pem** ファイルを作成します。

次の手順に従います。

► 次のディレクトリに切り替えます。

<ServerView ディレクトリ >\jboss\standalone\svconf\pki.

► 次のコマンドを適用します。

```
openssl pkcs12 -in keystore.p12 -passin pass:changeit
-nodes -out keystore.pem -passout pass:changeit
```

► **keystore.pem** ファイルを CMS の次のディレクトリにコピーします。

<ServerView directory>\jboss\standalone\svconf\pki

g) PEM 形式の **< システム名 >.scs.pem** ファイルを作成します。

次の手順に従います。

► 次のコマンドを適用します。

```
openssl pkcs12 -in keystore.p12 -passin pass:changeit -
out < システム名 >.scs.pem -passout pass:changeit
```

► 作成された証明書 **< システム名 >.scs.pem** を CMS の以下のディレクトリにコピーします。

<ServerView ディレクトリ >¥svcommon¥data¥download¥pki

このために、以下のコマンドを適用します。

```
COPY <system_name>.scs.pem
"<ServerView directory>\svcommon\data\download\pki\
<system_name>.scs.pem"
```

► ServerView エージェントが CMS にインストールされている場合 :

作成された証明書 **< システム名 >.scs.pem** を管理用サーバの以下のディレクトリにもコピーします。

<ServerView ディレクトリ >\Remote Connector\pki

CMS に同じ名前の既存の証明書がある場合は、置換されます。

7. JBoss サービスと ServerView サービスを再起動して、変更を有効にします。

4.2.4.2 Linux システムでの証明書の交換

次の手順に従います。

1. JBoss サービスを停止します（18 ページを参照）。
2. **keystore** ファイルを削除します。
   a) xterm ターミナルや gnome ターミナルなどの、ターミナルを開きます。
   b) **/opt/fujitsu/ServerViewSuite/jboss/standalone/svconf/pki** ディレクトリに移動します。
   c) **keystore** ファイルを削除するかファイル名を変更します。
3. CA が署名した証明書応答（ここでは **certreply.pem**）と CA 独自の証明書（ここでは certca.pem）を新しい **keystore** ファイルにインポートして、公開鍵（ここでは **keystore.p12**）をエクスポートします。

```
openssl pkcs12 -export -chain -in certreply.pem -inkey
privkey.pem -passout pass:changeit -out keystore.p12
-name "svs_cms" -CAfile certca.pem -caname "%CANAME%"
```

   i プレースホルダ %CANAME% を、証明書要求に署名した CA の名前に置き換えます。

4. **keystore** ファイルを（再）フォーマットします。

```
keytool -importkeystore -srckeystore keystore.p12
    -destkeystore keystore -srcstoretype PKCS12
    -srcstorepass changeit -deststorepass changeit
    -destkeypass changeit -srcalias svs_cms
    -destalias svs_cms -noprompt -v
```

5. 新しい証明書を **truststore** ファイルにインポートします。

   これを最も容易に行うには以下の手順に従います。

   a) JBoss サービスを開始します。
   b) スタートアップが完了するまで待ちます。
   c) **..\..\bin** ディレクトリに移動します。

d) ターミナルウィンドウを開いて以下のコマンドを入力します。

```
java -jar install-cert-gui-SVCOM_V1.70.jar
../conf/pki/cacerts changeit <system FQDN>:3170
```

i 設定済みの外部ディレクトリサービス（Active Directory など）を使用する場合は、次のコマンドも入力する必要があります。

```
java -jar install-cert-gui-SVCOM_V1.70.jar
../conf/pki/cacerts changeit <system FQDN>:<port>
```

< システム FQDN>
各システムの完全修飾識別名です。

<port>
外部ディレクトリサービスに使用される LDAP ポート（通常：636）

e) Java プログラム **install-cert-gui-SVCOM_V1.70.jar** により、次のようなパネルが表示されます。

図 31: Add Security Exception

このパネルを使用して、truststore にインポートする認証パス（Certificate Chain）から証明書を選択できます。エントリが 1 つしかない場合、証明書は自己署名式なので、これをインポートする以外に選択肢はありません。そうでない場合、上記例のように証明書が少なくとも 2 つになります。

1. サーバ証明書
2. サーバ証明書に署名した認証局（Certificate Authority : CA）の証明書

一般には、CA 証明書のみのインポートが推奨されます。その結果、同じ CA に署名されたサーバ証明書が自動的に信頼され、多くの場合有効です。

> **i** Java プログラムを呼び出すと、次のメッセージが表示されます
>
> ```
> testConnection(tm,pontresina.servware.abg.firm.net,
> 3170): SSLException: java.lang.RuntimeException:
> Unexpected error:
> java.security.InvalidAlgorithmParameterException: the
> trustAnchors parameter must be non-emptywriting to
> truststore ..\svconf\pki\cacerts...
> ```
>
> これはエラーではなく、新しい証明書がまだ **truststore** ファイルにインポートされていないことを示しているだけです。

f) PEM 形式の **keystore.pem** ファイルを作成します。

次の手順に従います。

► 次のコマンドを適用します。

```
openssl pkcs12 -in keystore.p12 -passin pass:changeit
-nodes -out keystore.pem -passout pass:changeit
```

► テキストエディタで **keystore.pem** ファイルを開き、以下以外のすべてのテキスト行を削除します。

– 「-----」の印のついたヘッダーおよびフッター
– 暗号化されたデータブロック行

► **keystore.pem** ファイルを CMS の次のディレクトリにコピーします。

/opt/fujitsu/ServerViewSuite/jboss/standalone/svconf/pki

g) CA 証明書は、**< システム名 >.scs.pem** として CMS の次のディレクトリにコピーする必要があります。

/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki

次の手順に従います。

► 次のコマンドを適用します。

```
cp certca.pem
/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki/
<system_name>.scs.pem
```

6. JBoss サービスを再起動して、変更を有効にします。

4.3 RBAC およびクライアント認証用の管理対象ノードの準備

RBAC およびクライアント認証用の管理対象ノードの準備には、次の手順が必要です。

1. 証明書ファイル（**< システム名 >.scs.pem** および **< システム名 >.scs.xml**）を管理対象ノードに転送します。
2. 転送したファイルを管理対象ノードにインストールします。

4.3.1 < システム名 >.scs.pem および < システム名 >.scs.xml の管理対象ノードへの転送

CMS での Operations Manager セットアップが正常に終了すると、**< システム名 >.scs.pem** および **< システム名 >.scs.xml** は CMS の次のディレクトリに保存されます。

– **<ServerView ディレクトリ >¥svcommon¥data¥download¥pki**（Windows システムの場合）

– **/opt/fujitsu/ServerViewSuite/svcommon/data/download/pki**（Linux システムの場合）

管理対象ノードは手動で転送できますが、CMS からダウンロードするほうが容易です。

ファイルをダウンロードするための要件 :

管理対象ノードで Web ブラウザが使用できること。

ファイルをダウンロードするには、次の手順に従います。

1. 管理対象ノードのブラウザで、次の URL を入力します。

   https://<system_name>:3170/Download/pki/

   > **重要**
   >
   > URL の末尾はスラッシュ（/）にする必要があります。

   < システム名 >

   < システム名 > には CMS の DNS 名または IP アドレスを入力します。

   次のウィンドウが開き、ダウンロードの用意ができているファイルが表示されます。

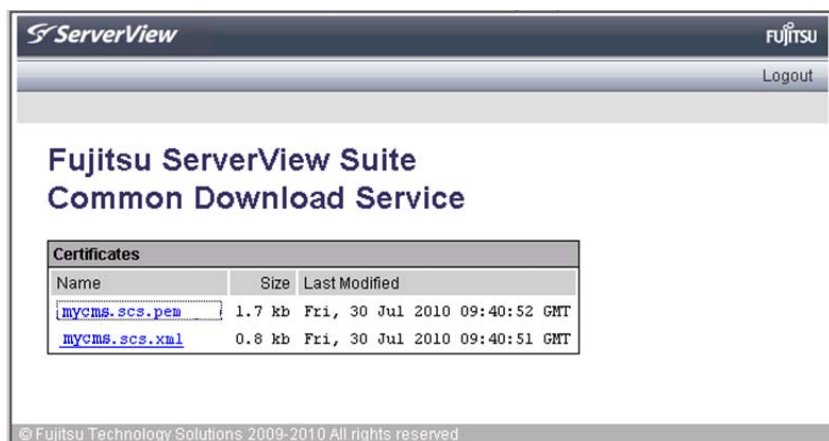



図 32: CMS mycms からの mycms.scs.pem および mycms.scs.xml のダウンロード

2. 各ファイルの対応するリンクを右クリックして、**対象をファイルに保存**を選択してファイルを管理対象ノードに保存します。

   > 「**対象をファイルに保存**」で、**.pem** ファイルを **.html** ファイルとして保存できます。この場合、ファイルのサフィックスを手動で **.html** から **.pem** に変更して、ファイルを使用できるようにしてください。

4.3.2 Windows システムでの証明書ファイルのインストール

証明書ファイル **< システム名 >.scs.pem** および **< システム名 >.scs.xml** のインストールには、以下のオプションがあります。

– ServerView エージェントと共に証明書ファイルを初期インストールする。

– 証明書ファイルを ServerView エージェントがすでにインストールされている管理対象ノードにインストールする（CMS で対応する交換を行ったために、最初にインストールした自己署名証明書を信頼される CA の証明書に交換しなければならない場合など）。

4.3.2.1 ServerView エージェントと共に証明書ファイルをインストールする

i この場合、ServerView エージェントを実際にインストールする前に、証明書ファイルを管理対象ノードにインストールします。

次に、Windows システムでの証明書ファイルのインストール方法を説明します。ServerView エージェントのインストール方法の詳細については、『ServerView Agents for Windows』マニュアルの該当する項を参照してください。

圧縮されたセットアップを使用するインストール

次の手順に従います。

1. 圧縮されたエージェントセットアップファイル（**ServerViewAgents_Win_i386.exe** または **ServerViewAgents_Win_x64.exe**）をネットワーク共有または管理対象ノードのローカルディレクトリにコピーします。

2. セットアップファイルを含むディレクトリで、新しいディレクトリ **pki**（公開鍵インフラストラクチャの略）を作成します。

3. 証明書ファイル **< システム名 >.scs.pem** および **< システム名 >.scs.xml** を新しい **pki** ディレクトリに転送します。複数の証明書を複数の信頼される CMS に転送することもできます。

4. 圧縮されたセットアップを実行します（詳細は『ServerView Agents for Windows』を参照）。ServerView エージェントのセットアップ時に、**pki** ディレクトリのすべての証明書が適切な場所にインストールされます。

解凍されたセットアップを使用するインストール

次の手順に従います。

1. 解凍されたセットアップファイル **ServerViewAgents_Win_i386.exe** または **ServerViewAgents_Win_x64.exe** をネットワーク共有または管理対象ノードのローカルディレクトリにコピーします。

   Setup.exe、**ServerViewAgents_xxx.msi** およびその他のファイルが作成されます。

2. セットアップファイルを含むディレクトリで、新しいディレクトリ **pki**（公開鍵インフラストラクチャの略）を作成します。

3. 証明書ファイル **<system_name>.scs.pem** および **<system_name>.scs.xml** を新しい **pki** ディレクトリに転送します。複数の証明書を複数の信頼される CMS に転送することもできます。

4. **Setup.exe** を実行します（詳細は『ServerView Agents for Windows』を参照）。ServerView エージェントのセットアップ時に、**pki** ディレクトリのすべての証明書が適切な場所にインストールされます。

ServerView Suite DVD からのインストール

> **i** ServerView エージェントおよび証明書は、ServerView Suite DVD から直接インストールできません。

次の手順に従います。

1. 圧縮または解凍されたエージェントセットアップファイルを、ServerView Suite DVD からネットワーク共有または管理対象ノードのローカルディレクトリにコピーします。

2. セットアップファイルを含むディレクトリで、新しいディレクトリ **pki**（公開鍵インフラストラクチャの略）を作成します。

3. 証明書ファイル **<system_name>.scs.pem** および **<system_name>.scs.xml** を新しい **pki** ディレクトリに転送します。複数の証明書を複数の信頼される CMS に転送することもできます。

4. 圧縮されたセットアップを実行します（詳細は『ServerView Agents for Windows』を参照）。ServerView エージェントのセットアップ時に、**pki** ディレクトリのすべての証明書が適切な場所にインストールされます。

4.3.2.2 ServerView エージェントがすでにインストールされている Windows システムでの証明書ファイルのインストール

次の手順に従います。

1. 管理対象ノードで ServerView Remote Connector Service（SCS）へのパス（以下 **<scsPath>** と略記）を探します。

   デフォルトのパスは次のとおりです。

   – x64 システムの場合 :

     C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥Remote Connector

   – i386 システムの場合 :

     C:¥Program Files¥Fujitsu¥ServerView Suite¥Remote Connector

2. 証明書ファイル **< システム名 >.scs.pem** および **< システム名 >.scs.xml** を SCS 証明書フォルダ **<scsPath>¥pki** に転送します。

   新しい証明書や変更された証明書は、10 秒以内、または Remote Connector Service の再起動後に SCS によってリロードされます。

4.3.3 Linux または VMware システムでの証明書ファイルのインストール

証明書ファイル **<system_name>.scs.pem** および **<system_name>.scs.xml** のインストールには、以下のオプションがあります。

– ServerView エージェントと共に証明書ファイルを初期インストールする。

– 証明書ファイルを ServerView エージェントがすでにインストールされている管理対象ノードにインストールする（CMS で対応する交換を行ったために、最初にインストールした自己署名証明書を信頼される CA の証明書に交換しなければならない場合など）。

4.3.3.1 ServerView エージェントと共に証明書ファイルをインストールする

i この場合、実際にシェルコマンドでインストールを開始する**前に**、証明書ファイルを管理対象ノードにインストールします。

i 次に、Linux または VMware システムでの証明書ファイルのインストール方法を説明します。ServerView エージェントのインストール方法の詳細については、『ServerView Agents for Linux』マニュアルの該当する項を参照してください。

ServerView Suite DVD からのインストール

1. **< システム名 >.scs.pem** および **< システム名 >.scs.xml** を **/temp** ディレクトリに転送します。
2. 次のコマンドを入力して環境変数 **SV_SCS_INSTALL_TRUSTED** をエクスポートします。

```
export SV_SCS_INSTALL_TRUSTED=/tmp
```

3. 次のコマンドを入力します。

```
sh srvmagtDVD.sh [-R]
```

   証明書ファイル **< システム名 >.scs.pem** および **< システム名 >.scs.xml** がインポートされます。

   新しい証明書や変更された証明書は、10 秒以内、または Remote Connector Service の再起動後に SCS によってリロードされます。

ディレクトリからのインストール

1. **< システム名 >.scs.pem** および **< システム名 >.scs.xml** を、ServerView エージェントのモジュールを含むローカルディレクトリに転送します。
2. 次のコマンドを入力します。

   ```
   sh ./srvmagt.sh [option] install
   ```

   証明書ファイル **<system_name>.scs.pem** および **<system_name>.scs.xml** がインポートされます。

rpm コマンドを使用するインストール

1. **< システム名 >.scs.pem** および **< システム名 >.scs.xml** をローカルディレクトリ **<cert dir>** に転送します。
2. 次のコマンドを入力して環境変数 **SV_SCS_INSTALL_TRUSTED** をエクスポートします。

   ```
   export SV_SCS_INSTALL_TRUSTED=<cert dir>
   ```

3. 次のコマンドを入力します。

   ```
   rpm -U ServerViewConnectorService-<scs-version>.i386.rpm
   ```

   証明書ファイル **<system_name>.scs.pem** および **<system_name>.scs.xml** がインポートされます。

4.3.3.2 ServerView エージェントがすでにインストールされている Linux/VMware システムでの証明書ファイルのインストール

次の手順に従います。

1. ターミナルを起動します（**root** として）。
2. 管理対象ノードで ServerView Remote Connector Service（SCS）へのパス（以下 **<scsPath>** と略記）を探します。

   デフォルトのパスは次のとおりです。

   /opt/fujitsu/ServerViewSuite/SCS/pki

3. **< システム名 >.scs.pem** および **< システム名 >.scs.xml** をローカルディレクトリに転送します。
4. 次のコマンドを入力します。

   ```
   cp -p <system_name>.scs.pem <system_name>.scs.xml <scsPath>
   ```

新しい証明書や変更された証明書は、10 秒以内、または Remote Connector Service の再起動後に SCS によってリロードされます。

4.3.4 ServerView Update Manager を使用する証明書のインストール（Windows/ Linux/VMware システム）

前提条件 :

ServerView Update エージェントおよび ServerView エージェントはバージョン 5.0 以降である必要があります。

サーバリストに表示される各管理対象ノードに対して、ServerView アップデートマネージャのアップデートメカニズムを使用して、CMS 証明書を管理対象ノードにサーバリストから直接インストールできます。他のアップデートコンポーネントの場合と同様に、アップデートマネージャにより、インストールに使用可能なソフトウェアとして CMS 証明書が提供されます。アップデートジョブを作成して開始することにより、証明書を管理対象ノードに自動的に転送できます。

この場合、CMS について生成された各証明書ファイルは、アップデートマネージャに割り当てられているリポジトリに置く必要があります（パス : **...\Tools\Certificates** (Windows) and **.../Tools/Certificates** (Linux / VMware):

– リポジトリの通常の初期設定では、アップデートマネージャの設定ウィザードにより、設定の最後に証明書がリポジトリに自動的に追加されます。

– アップデートインストール時に、該当するインストールスクリプトを実行することにより、証明書がリポジトリに自動的に追加されます。

重要 !

追加されるデータは各 CMS にのみ有効なため、ローカルリポジトリの指定しかできません。

4.3.4.1 管理対象ノードでの ServerView Update Manager を使用した CMS 証明書のインストール（概要）

下記の説明のようにアップデートマネージャのメインウィンドウを使用して、管理対象ノードでの CMS 証明書のインストールを制御できます。

アップデートマネージャの詳細は、『ServerView Update Manager』マニュアルを参照してください。

アップデートマネージャのメインウィンドウの「サーバ詳細」タブ（管理対象ノードに CMS 証明書をインストールする前）

CMS 証明書を管理対象ノードにインストールしない限り、「**サーバ詳細**」タブでこのノードの「**エージェントアクセス**」列に、「認証未」と表示されます（図 33 を参照）。

> **i** 管理対象ノードの ServerView Update エージェントおよび ServerView エージェントが 5.0 以降の場合、「**サーバ詳細**」タブでこのノードの「**エージェントアクセス**」列に、「制限」または「無制限」と表示されます。

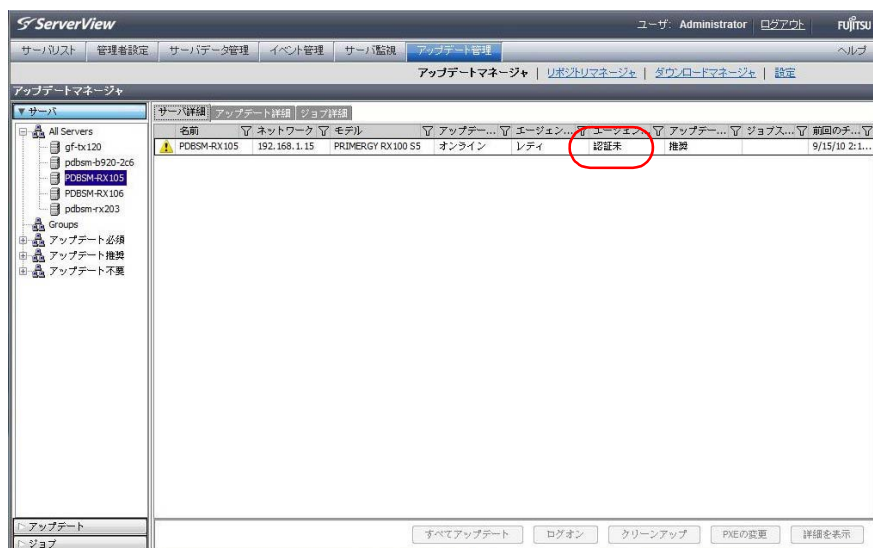



図 33: アップデートマネージャのメインウィンドウ - 「サーバ詳細」タブ（CMS 証明書がまだインストールされていない）

アップデートマネージャのメインウィンドウの「アップデート詳細」タブ（管理対象ノードに CMS 証明書をインストールする前）

「アップデート詳細」タブの「アップグレード」ビューでは、各行に選択したノードの CMS 証明書に関するインストールオプションが示されます（図 34 を参照）。

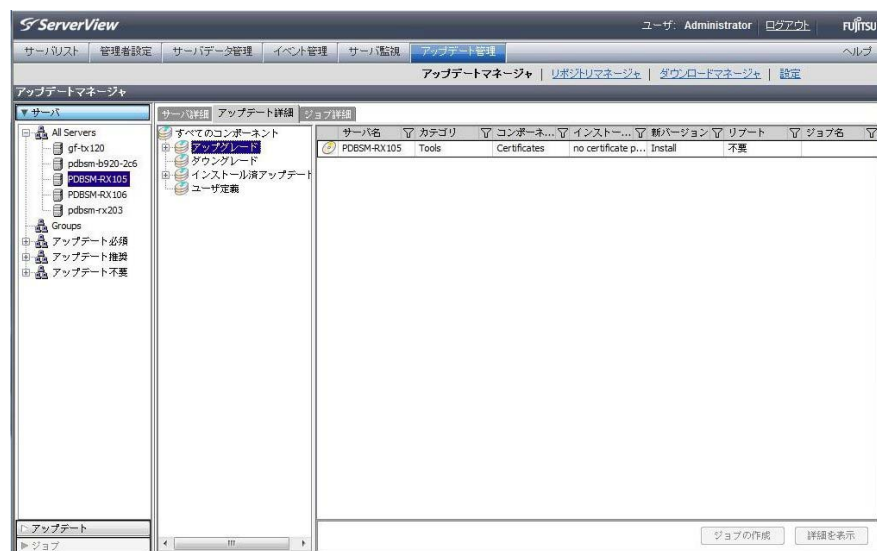



図 34: アップデートマネージャのメインウィンドウ - 「アップデート詳細」タブ（CMS 証明書がまだインストールされていない）

ここで、管理対象ノードでこのインストールを実行する新しいアップデートジョブを作成して開始できます。（アップデートジョブにはオプションで、その他のアップデートコンポーネントを追加できます）。アップデートジョブの作成方法の詳細は、『ServerView Update Manager』マニュアルを参照してください。

アップデートマネージャのメインウィンドウの「サーバ詳細」タブ（CMS ウィンドウで CMS 証明書が正常にインストールされた後）

CMS 証明書が正常にインストールされると、「**サーバ詳細**」タブでこのノードの「**エージェントアクセス**」列に、「認証済」と表示されます（図 35 を参照）。

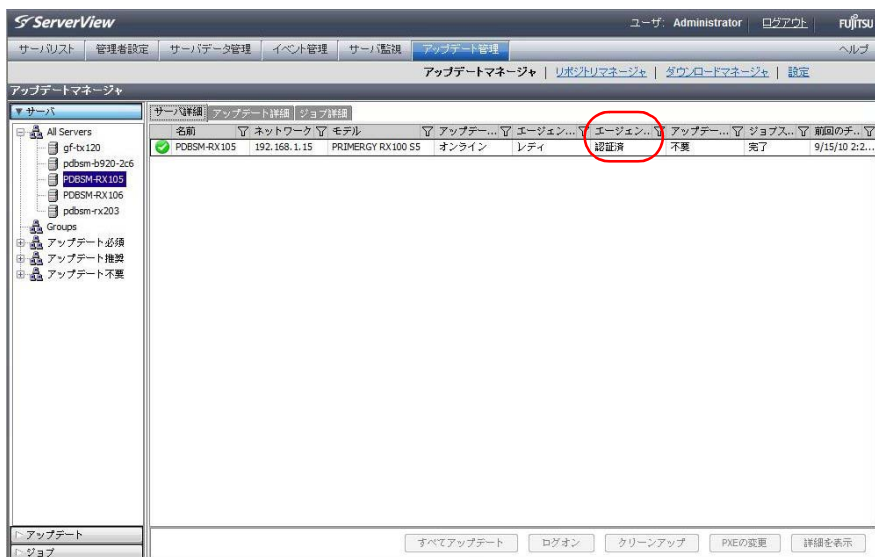



図 35: アップデートマネージャのメインウィンドウ - 「サーバ詳細」タブ（CMS 証明書が正常にインストールされた）

アップデートマネージャのメインウィンドウの「アップデート詳細」タブ（CMS ウィンドウで CMS 証明書が正常にインストールされた後）

CMS 証明書が管理対象ノードに正常にインストールされると、「**アップデート詳細**」タブの「**インストール済アップデート**」ビューに、CMS 証明書が管理対象ノードに正常にインストールされたことが示されます（図 36 を参照）。

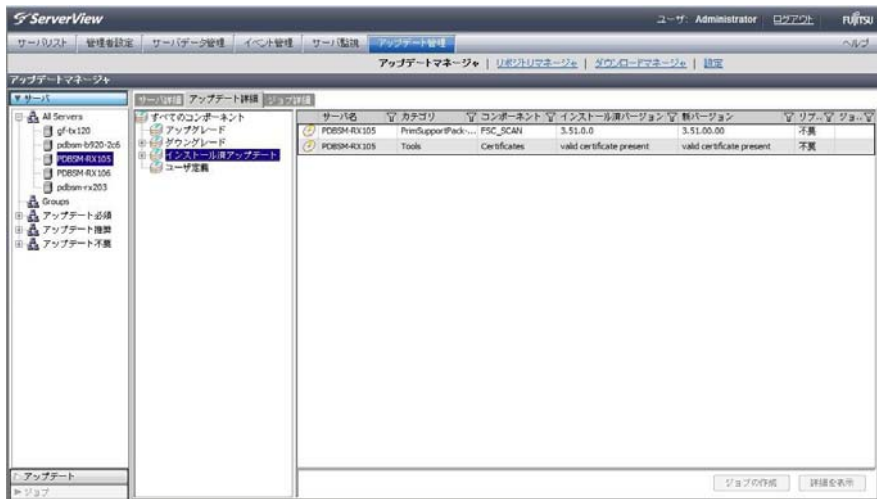



図 36: アップデートマネージャのメインウィンドウ - 「アップデート詳細」タブ（CMS 証明書が正常にインストールされた）

4.3.4.2 管理対象ノードでの CMS 証明書のインストール

管理対象ノードに CMS 証明書をインストールするには、次の手順に従います。

1. **アップデートマネージャ**のメインウィンドウを開きます（図 33 を参照）。
2. **すべてのサーバ**で、CMS 証明書をインストールする管理対象ノードを選択します。
3. 「**アップデート詳細**」タブの「**アップグレード**」ビュー（図 34 を参照）で、選択したノードの CMS 証明書に関するインストールオプションを示している行を選択します。
4. 管理対象ノードに CMS 証明書をインストールする新しいアップデートジョブを作成して開始します。

4.3.4.3 管理対象ノードからの CMS 証明書のアンインストール

管理対象ノードから CMS 証明書をアンインストールするには、次の手順に従います。

1. **アップデートマネージャ**のメインウィンドウを開きます（図 33 を参照）。
2. **すべてのサーバ**で、CMS 証明書をアンインストールする管理対象ノードを選択します。
3. 「**アップデート詳細**」タブの「**ダウングレード**」ビューで、「**新バージョン**」列に「Unstinstall」と表示される行を選択します（108 ページ の図 37 を参照）。
4. 管理対象ノードから CMS 証明書をアンインストールする新しいアップデートジョブを作成して開始します。

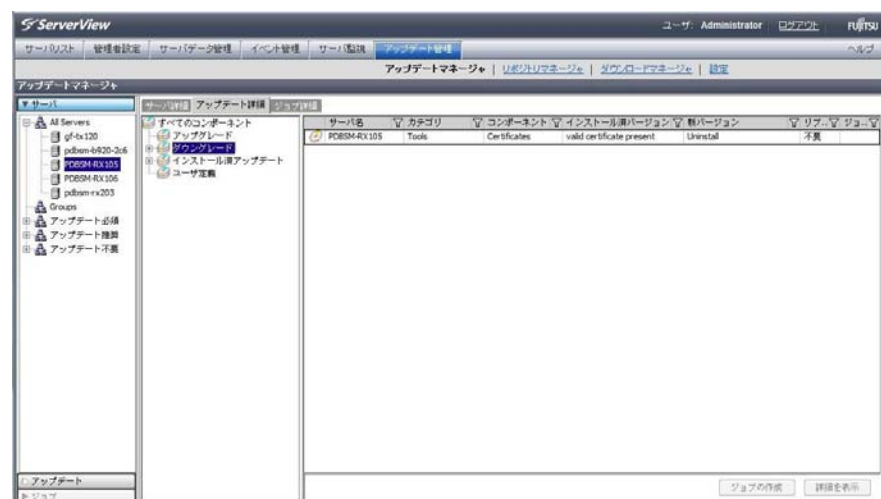



図 37: アップデートマネージャのメインウィンドウ - 「アップデート詳細」タブ（「ダウングレード」ビュー）

5 Operations Manager へのアクセスに関する役割ベースの許可

役割ベースのアクセス制御（RBAC）では、ユーザ役割（セキュリティ役割）に基づく権限を割り当てることにより、ユーザ権限を管理します。各役割を使用して、固有のタスク指向の権限プロファイルを定義できます。

ServerView Suite の RBAC 実装では権限がカテゴリに分類され、それぞれが固有の ServerView コンポーネントに対応します。

この章では以下について説明します。

– すべてのカテゴリと関連する権限

– 事前定義された役割 **Administrator**、**Monitor**、**Operator**、**UserAdministrator** および関連する権限

5.1 権限カテゴリと関連する権限

個々の ServerView コンポーネントを使用したり、ServerView 固有のタスクを実行したりできる権限は、権限カテゴリ（略してカテゴリと呼びます）に分類されます。各カテゴリは固有の ServerView コンポーネントに対応し、関連する ServerView コンポーネントを使用したりコンポーネント固有のタスクを実行したりできるすべての権限で構成されます。

5.1.1 権限カテゴリ（概要）

ServerView Suite では、次の権限カテゴリを使用できます。

権限カテゴリ	**関連する ServerView コンポーネント / タスク**
AgentDeploy	ServerView エージェントのデプロイ
AlarmMgr	アラーム管理
ArchiveMgr	アーカイブマネージャ
BackupMgr	データベースバックアップ
Common	一般的な ServerView Suite 固有の権限
ConfigMgr	Server Configuration Manager（SCU）およびリモート電源制御
InvMgr	インベントリマネージャ
iRMC_MMB	Baseboard Management Controller および BladeServer-MMB
PerfMgr	フォーマンスマネージャおよびスレッシュホールドマネージャ
PowerMon	パワーモニタ
RackManager	ラックマネージャ
RaidMgr	RAID マネージャ
RemDeploy	Deployment Manager および Installation Manager
ReportMgr	互換性の理由でのみサポートされます。
SCS	ServerView Connector Service
ServerList	サーバリスト
UpdMgr	アップデートマネージャ
UserMgr	ApacheDS でのユーザ管理
VIOM	Virtual IO Manager

表 4: 権限カテゴリおよび関連する ServerView コンポーネント / タスク

5.1.2 AgentDeploy カテゴリ

ServerView エージェントを管理対象ノードにデプロイするには、**AgentDeploy** カテゴリの **PerformAgentDeployment** 権限が必要です。

特権	**Permission**	**範囲**
PerformAgentDeployment	SV エージェントをノードにデプロイ。	CMS

表 5: AgentDeploy カテゴリの権限

5.1.3 AlarmMgr カテゴリ

AlarmMgr カテゴリは、ServerView イベント管理の各種タスクの実行に必要な権限で構成されます。

特権	**Permission**	**範囲**
AccessAlarmMgr	アラームモニタへのアクセス。	CMS
ModifyAlarmConfig	Operations Manager の開始ウィンドウの「**アラーム設定**」リンクを使用したアラーム設定の変更。 **注意 :** この権限は、**AccessServerList** 権限をすでに有するユーザにのみ割り当てられます。	CMS
PerformAlarmAcknowledge	アラームの確認。	全て
PerformMIBIntegration	新しい MIB の統合。	管理対象ノード

表 6: AlarmMgr カテゴリの権限

5.1.4 ArchiveMgr カテゴリ

ArchiveMgr カテゴリは、Archive Manager へのアクセス、およびアーカイブの作成、変更、削除に必要な権限で構成されます。

特権	Permission	範囲
AccessArchiveMgr	Archive Manager へのアクセス。	CMS
ModifyArchives	アーカイブを作成、変更、削除する	CMS

表 7: ArchiveMgr カテゴリの権限

5.1.5 BackupMgr カテゴリ

BackupMgr カテゴリは、Operations Manager Database のバックアップの管理に必要な権限で構成されます。

特権	Permission	範囲
ModifyBackup	Operations Manager Database のバックアップの作成 / 削除。	CMS
PerformBackupRestore	Operations Manager Database のリストア。	CMS
PerformBackupTransfer	Operations Manager Database のバックアップのアップロード / ダウンロード	CMS

表 8: BackupMgr カテゴリの権限

5.1.6 Common カテゴリ

Common カテゴリは、ServerView Suite 固有の共通タスクの実行に必要な権限で構成されます。

特権	**Permission**	**範囲**
AccessOnlineDiagnostics	管理対象ノードでのオンライン診断の開始。	管理対象ノード
AccessPrimeCollect	管理対象ノードでの PrimeCollect の開始。	管理対象ノード
AccessRemoteManagement	リモート管理ツールの開始。	全て
ConfigPKI	keystore または truststore の変更（証明初のインポートとエクスポート）。	全て
ModifyCMSSettings	CMS のローカル設定の変更。	全て
ModifyPasswordTable	パスワードテーブルの変更。	CMS
PerformDownload	ServerView インストールディレクトリから CMS へのデータのダウンロード。	CMS
PerformLocateToggle	識別灯の切り替え。	管理対象ノード
PerformServerErrorAck	サーバでのエラーの確認。	CMS

表 9: Common カテゴリの権限

5.1.7 ConfigMgr カテゴリ

ConfigMgr カテゴリは、Server Configuration Manager へのアクセスと使用に必要な権限、および Operations Manager のリモート電源制御機能に必要な権限で構成されます。

特権	**Permission**	**範囲**
AccessServerConfig	Server Configuration Manager へのアクセス。	全て
ModifyPowerOnOffSettings	シャットダウンコマンドの実行およびシャットダウン設定の変更。	全て
ModifyServerConfig	Server Configuration Manager を使用した管理対象ノードのサーバ設定の変更。	全て

表 10: ConfigMgr カテゴリの権限

5.1.8 InvMgr カテゴリ

InvMgr カテゴリは、Inventory Manager へのアクセスと、DataCollections および Reports の作成 / 変更 / 削除 / 実行に必要な権限で構成されます。

特権	**Permission**	**範囲**
AccessInvMgr	Inventory Manager へのアクセス。	CMS
ModifyCollections	DataCollections および関連する定義の作成、変更、削除。	CMS
ModifyDiagnostics	タスク関連のログおよびエクスポートデータの表示および削除。	CMS
ModifyReports	Reports および関連する定義の作成、変更、削除。	CMS
PerformCollections	DataCollections の実行。	CMS
PerformReports	Reports の実行。	CMS

表 11: InvMgr カテゴリの権限

5.1.9 iRMC_MMB カテゴリ

iRMC_MMB カテゴリは、iRMC S2/S3/S4 / MMB へのアクセスと使用に必要な権限で構成されます。

注意事項 :

「Ipmi」というプレフィックスで始まる権限は、IPMI 仕様に規定される権限に基づいています。IPMI の下では、ユーザ設定はチャネル固有です。したがって、ユーザは iRMC S2/S3/S4 / MMB に LAN チャネル経由でアクセスしているか、シリアルチャネル経由でアクセスしているかに応じて、異なる権限を持つことができます。

各ユーザ / 役割には､Ipmi Lan 権限レベルと Ipmi Serial 権限レベルを 1 つずつ指定する必要があります。

特権	**Permission**	**範囲**
CfgConnectionBlade	Connection Blade を設定する権限。	管理対象ノード
IpmiLanOem	すべての LAN 接続における OEM 固有の IPMI 権限レベル **OEM**。**OEM** レベルには、標準 IPMI 権限レベル **administrator** が含まれ、さらに OEM 機能を実行可能。	管理対象ノード
IpmiLanOperator	すべての LAN 接続における標準 IPMI 権限レベル **operator**。	管理対象ノード
IpmiLanUser	すべての LAN 接続における標準 IPMI 権限レベル **user**。	管理対象ノード
IpmiSerialOem	すべてのシリアル接続における OEM 固有の IPMI 権限レベル **OEM**。**OEM** レベルには、標準 IPMI 権限レベル **administrator** が含まれ、さらに OEM 機能を実行可能。	管理対象ノード
IpmiSerialOperator	すべてのシリアル接続における標準 IPMI 権限レベル **operator**。	管理対象ノード
IpmiSerialUser	すべてのシリアル接続における標準 IPMI 権限レベル **user**。	管理対象ノード
iRMCsettings	iRMC S2/S3/S4 設定（構成）を変更する権限。	管理対象ノード
RemoteStorage	iRMC S2/S3/S4 の **リモートストレージ** 機能を使用する権限。	管理対象ノード
UserAccounts	iRMC S2/S3/S4 / MMB のローカルデータベースでユーザアカウントを作成、削除、変更する権限。	管理対象ノード

表 12: iRMC_MMB カテゴリの権限

特権	Permission	範囲
VideoRedirection	iRMC S2/S3/S4 を使用してビデオリダイレクションセッションを開く権限。	管理対象ノード

表 12: iRMC_MMB カテゴリの権限

5.1.10 PerfMgr カテゴリ

PerfMgr カテゴリは、パフォーマンスマネージャおよびスレッシュホールドマネージャへのアクセスと使用に必要な権限で構成されます。

特権	Permission	範囲
AccessPerformanceMgr	パフォーマンスマネージャへのアクセス。	CMS
AccessThresholdMgr	スレッシュホールドマネージャへのアクセス。 **注意 :** この権限は、**AccessServerList** 権限をすでに有するユーザにのみ割り当てられます。	CMS

表 13: PerfMgr カテゴリの権限

5.1.11 PowerMon カテゴリ

The **PowerMon** カテゴリの **AccessPowerMonitor** 権限は、パワーモニタへのアクセスと使用に必要です。

特権	Permission	範囲
AccessPowerMonitor	パワーモニタへのアクセス。	CMS

表 14: PowerMon カテゴリの権限

5.1.12 RackManager カテゴリ

RackManager カテゴリは、ラックマネジメントに関連するアクティビティに必要な権限で構成されます。

特権	Permission	範囲
AccessRack	ラックグループの表示（管理機能とも呼ばれる）。	全て
AccessUserGroup	ユーザ定義グループの表示。	全て
ModifyRack	ラック位置の編集。割り当てられていないシステムのラックへの分類。	全て
ModifyTask	新規タスクの作成。	全て
ModifyUserGroup	ユーザ定義グループの作成と変更。	全て

表 15: RackManager カテゴリの権限

5.1.13 RaidMgr カテゴリ

RaidMgr カテゴリは、RAID Manager へのアクセスと、RAID 構成の変更に必要な権限で構成されます。

特権	Permission	範囲
AccessRaidMgr	RAID Manager へのアクセス（読み取りアクセス）。	全て
ModifyRaidConfig	RAID 構成の変更 （読み取り / 書き込みアクセス）。	全て

表 16: RaidMgr カテゴリの権限

5.1.14 RemDeploy カテゴリ

RemDeploy カテゴリは、インストールおよびデプロイアクティビティの実行に必要な権限で構成されます。

特権	Permission	範囲
AccessDeploymentMgr	Installation Manager へのアクセス。	CMS
AccessDeploymentMgr2	Deployment Manager へのアクセス。	CMS
ModifyDmNode	サーバの作成、変更、削除。Deployment Configuration のエクスポートとインポート。	全て
ModifyDmSettings	Deployment Manager のグローバル設定の変更。	全て
PerformDmCreateImage	サーバのクローニングイメージまたはスナップショットイメージの作成。	全て
PerformDmDeployImage	サーバへのクローニングイメージまたはスナップショットイメージのリストア。	全て
PerformDmInstallServer	サーバのインストール。	全て
PerformDmPowerOperations	システムの電源のオン / オフ。	全て

表 17: RemDeploy カテゴリの権限

5.1.15 ReportMgr カテゴリ

ReportMgr カテゴリと関連する **AccessReportMgr** 権限は、互換性の理由でのみサポートされます。そのため、無視してかまいません。

特権	Permission	範囲
AccessReportMgr	レポートマネージャへのアクセス。	CMS

表 18: ReportMgr カテゴリの権限

5.1.16 SCS カテゴリ

SCS カテゴリの **ModifyTrustedHosts** 権限は、信頼できるホスト設定の変更に必要です。

特権	Permission	範囲
ModifyTrustedHosts	信頼できるホスト設定の変更。 **注意 :** この権限は、**ConfigPKI** 権限をすでに有するユーザにのみ割り当てることができます。	管理対象ノード

表 19: SCS カテゴリの権限

5.1.17 ServerList カテゴリ

ServerList カテゴリは、ServerList へのアクセスと関連する操作に必要な権限で構成されます。

特権	Permission	範囲
AccessServerList	ServerList へのアクセス（すべてのシステムのシングルシステムビューへの暗黙的なアクセス権限を含む）。	CMS
ModifyNode	サーバおよびグループの作成、変更、削除。	CMS
PerformArchiveImport	アーカイブのインポート。	CMS
PerformConnectivityTest	接続テストの実行。	CMS
PerformDiscovery	ノード（サーバなど）の検出とサーバブラウザへのアクセス。 **注意 :** この権限は、**PerformConnectivityTest** および **ModifyNode** 権限をすでに有するユーザにのみ割り当てることができます。	CMS
PerformExploration	ノードでの「エクスプローラ」タスクの開始。 **注意 :** この権限は、**ModifyNode** 権限をすでに有するユーザにのみ割り当てることができます。	CMS
PerformPowerOperations	電源のオン / オフ。システムのリブート。	CMS

表 20: ServerList カテゴリの権限

5.1.18 UpdMgr カテゴリ

UpdMgr カテゴリは、ServerView Download Manager / Repository Manager / Update Manager へのアクセスと、対応するアップデート管理関連タスクの実行に必要な権限で構成されます。

特権	Permission	範囲
AccessDownloadMgr	Download Manager へのアクセス。	CMS
AccessRepositoryMgr	リポジトリマネージャへのアクセス。	CMS
AccessUpdateMgr	アップデートマネージャへのアクセス。	CMS
DeleteJob	ジョブの削除。	CMS
DeleteReleasedJob	リリースされたジョブの削除。	CMS
ModifyUpdateConfig	アップデート設定へのアクセス。	CMS
PerformCleanUp	管理対象ノードでの、Update エージェントのデータのクリーンアップ。	CMS
PerformCopyJob	ファームウェア / ソフトウェアアップデートでのジョブのコピー。	CMS
PerformCopyReleasedJob	リリースされたジョブのコピー。	CMS
PerformCreateJob	ファームウェア / ソフトウェアアップデートでのジョブの作成。	CMS
PerformReleaseJob	ジョブのリリース。	CMS

表 21: UpdMgr カテゴリの権限

5.1.19 UserMgr カテゴリ

UserMgr カテゴリは、「ユーザ管理」ウィザードへのアクセスと、それを使用して以下のタスクを実行するために必要な権限で構成されます。

– ユーザの作成、変更、削除。
– 役割の定義と変更。
– ユーザへの役割の割り当て。

特権	**Permission**	**範囲**
AccessUserMgr	**「ユーザ管理」**ウィザードへのアクセス。	CMS
PerformUserMgt	**「ユーザ管理」**ウィザードを使用して ApacheDS でのユーザ管理を実行。	CMS

表 22: UserMgr カテゴリの権限

5.1.20 VIOM カテゴリ

VIOM カテゴリの **AccessVIOM** 権限は、ServerView Virtual-IO Manager（VIOM）へのアクセスに必要です。

特権	**Permission**	**範囲**
AccessVIOM	VIOM へのアクセス。	全て

表 23: VIOM カテゴリの権限

5.2 ApacheDS で事前定義されているユーザと役割

ApacheDS では、ユーザ役割の **Administrator**、**Monitor**、**Operator**、**UserAdministrator** が事前定義されており、事前定義されたユーザの **Administrator**、**Monitor**、**UserManager** にそれぞれ永続的に割り当てられています。

次の表に、事前定義された役割によって承認される権限を示します。

カテゴリ	特権	事前定義されているユーザ / 役割			
		Administrator / Administrator	Operator / Operator	Monitor / モニタ	UserManager/ UserAdministrator
AgentDeploy	PerformAgentDeployment	X	-	-	-
AlarmMgr	AccessAlarmMgr	X	X	X	-
	ModifyAlarmConfig	X	-	-	-
	PerformAlarmAcknowledge	X	X	-	-
	PerformMIBIntegration	X	X	-	-
ArchiveMgr	AccessArchiveMgr	X	X	-	-
	ModifyArchives	X	X	-	-
BackupMgr	ModifyBackup	X	-	-	-
	PerformBackupRestore	X	-	-	-
	PerformBackupTransfer	X	-	-	-

表 24: 事前定義された役割によって承認される権限

カテゴリ	特権	事前定義されているユーザ / 役割			
		Administrator / Administrator	Operator / Operator	Monitor / モニタ	UserManager/ UserAdministrator
Common	AccessOnlineDiagnostics	X	X	-	-
	AccessPrimeCollect	X	X	X	-
	AccessRemoteManagement	X	X	-	-
	ConfigPKI	X	-	-	-
	ModifyCMSSettings	X	-	-	-
	ModifyPasswordTable	X	-	-	-
	PerformDownload	X	X	-	-
	PerformLocateToggle	X	X	-	-
	PerformServerErrorAck	X	X	-	-
ConfigMgr	AccessServerConfig	X	-	-	-
	ModifyPowerOnOffSettings	X	X	-	-
	ModifyServerConfig	X	-	-	-
InvMgr	AccessInvMgr	X	X	-	-
	ModifyCollections	X	-	-	-
	ModifyDiagnostics	X	X	-	-
	ModifyReports	X	-	-	-
	PerformCollections	X	X	-	-
	PerformReports	X	X	-	-
iRMC_MMB	CfgConnectionBlade	X	-	-	-
	IpmiLanOem	X	-	-	-
	IpmiLanOperator	-	X	-	-
	IpmiLanUser	-	-	X	-
	IpmiSerialOem	X	-	-	-
	IpmiSerialOperator	-	X	-	-
	IpmiSerialUser	-	-	X	-
	iRMCsettings	X	-	-	-

表 24: 事前定義された役割によって承認される権限

カテゴリ	特権	事前定義されているユーザ / 役割			
		Administrator / Administrator	Operator / Operator	Monitor / モニタ	UserManager/ UserAdministrator
	RemoteStorage	X	-	-	-
	UserAccounts	X	-	-	-
	VideoRedirection	X	X	-	-
PerfMgr	AccessPerformanceMgr	X	X	-	-
	AccessThresholdMgr	X	X	-	-
PowerMon	AccessPowerMonitor	X	X	X	-
RackManager	AccessRack	X	X	X	-
	AccessUserGroup	X	X	X	-
	ModifyRack	X	X	-	-
	ModifyTask	X	-	-	-
	ModifyUserGroup	X	X	-	-
RaidMgr	AccessRaidMgr	X	X	X	-
	ModifyRaidConfig	X	X	-	-
RemDeploy	AccessDeploymentMgr	X	-	-	-
	AccessDeploymentMgr2	X	X	X	-
	ModifyDmNode	X	X	-	-
	ModifyDmSettings	X	-	-	-
	PerformDmCreateImage	X	X	-	-
	PerformDmDeployImage	X	-	-	-
	PerformDmInstallServer	X	-	-	-
	PerformDmPowerOperations	X	X	-	-
SCS	ModifyTrustedHosts	X	-	-	-

表 24: 事前定義された役割によって承認される権限

カテゴリ	特権	事前定義されているユーザ / 役割			
		Administrator / Administrator	Operator / Operator	Monitor / モニタ	UserManager/ UserAdministrator
サーバリスト	AccessServerList	X	X	X	-
	ModifyNode	X	X	-	-
	PerformArchiveImport	X	X	-	-
	PerformConnectivityTest	X	X	X	-
	PerformDiscovery	X	X	-	-
	PerformExploration	X	X	-	-
	PerformPowerOperations	X	X	-	-
UpdMgr	AccessDownloadMgr	X	-	-	-
	AccessRepositoryMgr	X	-	-	-
	AccessUpdateMgr	X	X	-	-
	DeleteJob	X	-	-	-
	DeleteReleasedJob	X	X	-	-
	ModifyUpdateConfig	X	-	-	-
	PerformCleanUp	X	-	-	-
	PerformCopyJob	X	-	-	-
	PerformCopyReleasedJob	X	X	-	-
	PerformCreateJob	X	-	-	-
	PerformReleaseJob	X	-	-	-
UserMgr	AccessUserMgr	-	-	-	X
	PerformUserMgt	-	-	-	X
VIOM	AccessVIOM	X	-	-	-

表 24: 事前定義された役割によって承認される権限

6　監査ログ

監査ログでは、IT システム内の任意のアクションを IT システムの責任者に割り当てることができます。エラーログと異なり、監査ログは成功したアクションの記録に重点が置かれます。監査ログを行う目的は、システムの監視ではありません。監査ログにより、権限保持者は後でシステム（リビジョン）でのプロセスを評価できます。監査ログ時に記録されたエントリは長期間保持されます。長期間経過してもエントリを正しく解釈できるように、記録フォーマットの説明も監査ログと共に保持する必要があります。ServerView では、コンポーネント固有のユーザアクションログを提供します。

i　現時点では、監査ログのエントリを作成する ServerView コンポーネントは Central Authentication Service（CAS）のみです。

6.1　監査ログの保存場所

Windows システムでの監査ログの保存情報

Windows システムでは、監査ログ情報はアプリケーションイベントログに書き込まれます。

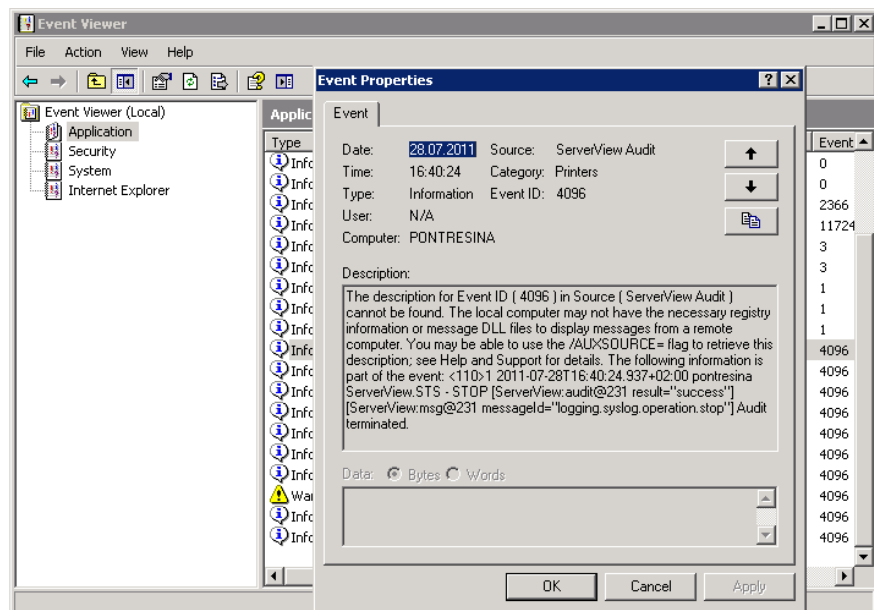



図 38: ServerView 監査ログは、Windows アプリケーションイベントログの一部です。

Linux システムでの監査ログの保存情報

Linux システムでは、監査ログ情報は、**/var/log/fujitsu/ServerViewSuite/jboss** ディレクトリにある UTF-8 でエンコードされたファイル **audit.log** に書き込まれます。**audit.log** ファイルは毎日新しく作成されます。現在の **audit.log** ファイルの前のファイルの名前は、**audit.log.<YYYY-MM-DD>.log** に変更されます。ここで、**<YYYY-MM-DD>** は、前日の各日付です。

6.2 監査ログエントリ

監査ログファイルの各行が、1 つの監査ログエントリになります。監査ログファイルのエントリの構造は、RFC 5424（Syslog プロトコル）に基づいています。

各ログエントリは、ヘッダーとそれに続く構造化データで構成されます。

– ヘッダーは、各エントリにあるフィールドのリストです。

– 構造化データ（RFC 5424 の STRUCTURED-DATA）は、ログに記録されたアクションの詳細を示します。

i

– 構文要素の詳細は、RFC 5424 で参照できます。

– ログエントリの例は、137 ページ の「例 : 監査ログファイルのエントリ」の項を参照してください。

6.2.1 監査ログエントリのタイプ

監査ログエントリには 3 つのタイプがあります。

- INIT エントリ

  INIT エントリは常に監査ログファイルの最初のエントリで、次のように構造化されています。

  – ヘッダー
  – ServerView:audit@231 要素
  – origin 要素
  – ServerView:env@231 要素
  – 構造化データに続くフリーテキスト

- <operation> エントリ

  <operation> エントリは、<COMP_Name> で指定された ServerView コンポーネントで実行された操作 <operation> を指します。

  <operation> エントリは次のように構造化されています。

  – ヘッダー
  – ServerView.<COMP_Name>:audit@231 要素
  – 構造化データに続くフリーテキスト

- STOP エントリ

  STOP エントリは通常、監査ログファイの最後のエントリで、次のように構造化されています。

  – ヘッダー
  – ServerView:audit@231 要素
  – 構造化データに続くフリーテキスト

  i ログに記録されたコンポーネントが異常終了した場合、STOP エントリがないことがあります。

以下の項では、上記で説明した監査ログエントリコンポーネント（ヘッダー、要素）の詳細を説明します。

6.2.2 監査ログエントリのヘッダー

ヘッダーには次のフィールドがあり、それぞれスペースで区切られています。

フィールドの内容	説明
<108>1 / <110>1	RFC 5424 に準拠し、これらの番号の意味は次のとおりです。 <108> 1 は <(**13** * 8) + **4**> **1** で計算され、詳細は以下のとおりです。 Syslog ファシリティ : **13**（ログ監査） Syslog 重要度 : **4**（警告） Syslog プロトコル : バージョン **1** <110> 1 は <(**13** * 8) + **6**> **1** で計算され、詳細は以下のとおりです。 Syslog ファシリティ : **13**（ログ監査） Syslog 重要度 : **6**（情報） Syslog プロトコル : バージョン **1**
タイムスタンプ	イムスタンプは、RFC 3339 で規定される形式に従います。
コンピュータ名	コンピュータ名
ServerView コンポーネント	ServerView コンポーネントの名前。現時点では、ログエントリを書き込む ServerView コンポーネントは `ServerView.CAS` のみです。
-	各行における定数。プロセス ID は記録されません（RFC 5424 の規定）。
MsgId	印刷可能な形式の、操作の名前。バージョン 3 の Server エントリでは、これは ServerView コンポーネントの操作です。

表 25: 監査ログエントリのヘッダー

例

<110>1	2011-07-07T09:42:03.113+02:00	compA1	ServerView.CAS	-	LOGIN

6.2.3 監査ログエントリの構造化データ

監査ログエントリのヘッダーには、イベントを記述する構造化データが後続します。構造化データは、要素（RFC 5424 の SD-ELEMENT）のリストで構成され、各要素は角括弧（[ ]）で囲まれています。角括弧の中では、各要素の要素名（RFC 5424 の SD-NAME）が先頭にあり、「キー /" 値 "」ペアの形式でパラメータのリストが後続します（RFC 5424 の SD-PARAM）。値はそれぞれ二重引用符（"）で囲まれています。要素の順序は指定されていません。提示される要素と値は対象となるイベントに応じて異なり、以下で詳細を説明します。監査ログエントリには次の要素が含まれ、`COMP_NAME` は対応するコンポーネント名を示します。

i 名前 `ServerView.COMP_NAME:audit@231` の要素は各エントリに含まれます。その他の要素はすべてオプションです。

6.2.3.1 origin 要素

origin 要素は、MsgId `INIT` を持つエントリに含まれています。要素名 **origin** とそのパラメータの意味は、Internet Assigned Numbers Authority（

IANA）によって RFC 5424 に登録されているため、サフィックス `@231` はありません。**origin** 要素には、どのベンダのどの製品がログエントリを作成したかという情報が含まれています。

パラメータ	意味
ソフトウェア	製品名（常に ServerView）とコンポーネント名（CAS など）。
swVersion	監査ログが作成された時点での ServerView コンポーネントのバージョン。
enterpriseId	会社について IANA に登録されているプライベートエンタープライズ番号。Fujitsu Technology Solutions のプライベートエンタープライズ番号は 231 です。

表 26: 監査ログエントリ - origin 要素

6.2.3.2 ServerView:env@231 要素

ServerView:env@231 要素は、Msgid `INIT` を持つログエントリに含まれています。ランタイム環境の情報が含まれています。

パラメータ	意味
javaHome	Java インストールディレクトリ
javaVendor	Java Runtime 環境ベンダ
jbossUserDir	JBoss ユーザの現在のワークディレクトリ
jbossUserHome	JBoss ユーザのホームディレクトリ
jbossUserName	JBoss ユーザのアカウント名
osName	オペレーティングシステム名
osVersion	オペレーティングシステムバージョン

表 27: 監査ログエントリ - ServerView:env@231 要素

6.2.3.3 ServerView:audit@231 要素

ServerView:audit@231 エントリは各監査ログエントリの一部です。「231」

は Internet Assigned Numbers Authority（IANA）に登録されている Fujitsu Technology Solutions のプライベートエンタープライズ番号です。サフィックス「@231」は、この要素が RFC 5424

に従って Fujitsu Technology Solutions に予約された要素であることを示します。

パラメータ	意味
result	操作が正常に実行されたかどうかを指定します。次の値が可能です。 「success」: 操作が実行されました。 「failure」: 操作が失敗しました。

表 28: 監査ログエントリ - ServerView:audit@231 要素

6.2.3.4 ServerView[.<COMP_NAME>]:msg@231 要素

ServerView[.<COMP_NAME>]:audit@231 エントリは各監査ログエントリの一部です。現在の操作を説明するメッセージに対応する ID が含まれています。

<COMP_NAME> は、監査ログエントリを発行する ServerView コンポーネントを示します。すべての ServerView コンポーネントに複数のメッセージが適用されます。この場合、名前の **.<COMP_NAME>** の部分は省略されます。「231」は Internet Assigned Numbers Authority（IANA）に登録されている Fujitsu Technology Solutions のプライベートエンタープライズ番号です。サフィックス @231 は、この要素が RFC 5424

に従って Fujitsu Technology Solutions に予約された要素であることを示します。

パラメータ	意味
messageId	現在の操作を説明するメッセージに対応するメッセージ ID。

表 29: 監査ログエントリ - ServerView[.<COMP_NAME>]:msg@231 要素

6.2.3.5 ServerView[.<COMP_NAME>]:<operation>@231 要素

この要素は ServerView コンポーネントに固有で、Msgid **<operation>** を持つ各監査ログエントリに 1 つ含まれます。この要素は操作要求の詳細を示します。

i 要素に含まれる正確なパラメータは、対応する操作とその結果に依存します。現在、監査ログをサポートする ServerView コンポーネトは Central Authentication Service（`COMP_NAME = CAS`）と Security Token Service
（`COMP_NAME = STS`）です。

ServerView コンポーネントの CAS と STS が作成した監査ログエントリの構造を、以下で説明します。

ServerView コンポーネント CAS

以下の監査ログエントリは、ユーザが ServerView セッションにサインオンしようとするたびに作成されます。

```
MSG-ID = LOGIN
SD-ID = ServerView.CAS:login@231
```

パラメータ	意味
アドレス	クライアントシステムの IP アドレス。
ユーザ	ログイン操作で指定されたユーザ ID。
tgt	ログイン操作で作成された CAS チケット認可チケット。

表 30: 監査ログエントリ - ServerView.CAS:login@231 のパラメータ

以下の監査ログエントリは、ユーザが ServerView セッションからサインアウトするたびに作成されます。

```
MSG-ID = LOGOUT
SD-ID = ServerView.CAS:logout@231
```

パラメータ	意味
アドレス	クライアントシステムの IP アドレス。
ユーザ	ログアウト操作で指定されたユーザ ID。
tgt	ログイン操作で作成された CAS チケット認可チケット。

表 31: 監査ログエントリ - ServerView.CAS:logout@231 のパラメータ

ServerView コンポーネント STS

以下の監査ログエントリは、STS クライアントが CAS チケット認可チケット（TGT）を含むバイナリセキュリティトークンを取得したときに作成されます。

```
MSG-ID = RST_ISSUE_TGT
SD-ID = ServerView.STS:rstIssueTgt@231
```

パラメータ	意味
アドレス	クライアントシステムの IP アドレス。
ユーザ	RST の「TGT 発行」要求のユーザ名トークンで指定されたユーザ ID。
tgt	RST 操作で作成された CAS チケット認可チケット。

表 32: 監査ログエントリ - ServerView.STS:rstIssueTgt@231 のパラメータ

以下の監査ログエントリは、STS クライアントが CAS サービスチケット（ST）を含むバイナリセキュリティトークンを取得したときに作成されます。

```
MSG-ID = RST_ISSUE_ST
SD-ID = ServerView.STS:rstIssueSt@231
```

パラメータ	意味
アドレス	クライアントシステムの IP アドレス。
tgt	RST 要求のバイナリセキュリティセキュリティトークで指定された、CAS チケット認可チケット。
st	RST の「ST 発行」要求で作成された CAS サービスチケット。

表 33: 監査ログエントリ - ServerView.STS:rstIssueSt@231 のパラメータ

以下の監査ログエントリは、STS クライアントが CAS サービスチケット（ST）を含むバイナリセキュリティトークンを取得したときに作成されます。

```
MSG-ID = VALIDATE
SD-ID = ServerView.STS:validate@231
```

パラメータ	意味
アドレス	クライアントシステムの IP アドレス。
st	RST の「ST 発行」要求で作成された CAS サービスチケット。
ユーザ	RST の「TGT 発行」要求のユーザ名トークンで指定されたユーザ ID。

表 34: 監査ログエントリ - ServerView.STS:validate@231 のパラメータ

6.2.4 例 : 監査ログファイルのエントリ

以下の例では、ServerView の Central Authentication Service（CAS）の監査ログエントリを示します。読みやすいように、改行を付加しています。

INIT エントリ

次の INIT エントリには、構造化データに続けて要素 origin、ServerView:audit@231、ServerView.CAS:env@231 とフリーテキストが含まれています。

```
<110>1 2011-07-20T08:33:16.265+02:00 pontresina
ServerView.CAS - INIT
[ServerView:audit@231 result="success"]
[ServerView:env@231 javaHome="C:\\Program Files\\Java\\jre7"
javaVendor="Sun Microsystems Inc." javaVersion="1.6.0_26"
jbossUserDir="C:\\Program Files\\Fujitsu\\ServerView
Suite\\jboss\\bin" jbossUserHome="D:\\Profiles\\jbossrun"
jbossUserName="jbossrun" osName="Windows XP" osVersion="5.1"]
[ServerView:msg@231 messageId="logging.syslog.operation.init"]
[origin enterpriseId="231" software="ServerView.CAS" swVersion=
"SVCOM_V1.50/3.3.2"] Audit started
```

LOGIN エントリ（失敗したログイン）

次の LOGIN エントリには、構造化データに続けて要素 ServerView:audit@231 とフリーテキストが含まれています。このエントリは、ログイン失敗によって発生した「警告」エントリを示します。

```
<108>1 2011-07-20T08:38:52.234+02:00 pontresina
ServerView.CAS - LOGIN
[ServerView.CAS:login@231 address="172.25.88.121"]
[ServerView.CAS:msg@231 messageId=
"error.authentication.credentials.bad"]
[ServerView:audit@231 result="failure"] The credentials you
provided cannot be determined to be authentic.
```

LOGIN エントリ（成功したログイン）

ログイン成功によって生成された次の LOGIN エントリには、構造化データに続けて要素 ServerView:audit@231 とフリーテキストが含まれています。

```
<110>1 2011-07-20T08:38:32.406+02:00 pontresina
ServerView.CAS - LOGIN
[ServerView.CAS:login@231 address="172.25.88.121" tgt=
"TGT-1-VSOg93zTt2dZQ1WX1texuXNEmJKvw21HelXqXIScvMKVi7XOBY-cas"
user="administrator"]
[ServerView.CAS:msg@231 messageId=
"screen.success.header"][ServerView:audit@231 result=
"success"]Log In Successful
```

LOGOUT エントリ

次の LOGOUT エントリには、構造化データに続けて要素 ServerView:audit@231 とフリーテキストが含まれています。

```
<110>1 2011-07-20T08:38:35.156+02:00 pontresina
ServerView.CAS - LOGOUT
[ServerView.CAS:logout@231 address="172.25.88.121" tgt=
"TGT-1-VSOg93zTt2dZQ1WX1texuXNEmJKvw21HelXqXIScvMKVi7XOBY-cas"
user="administrator"]
[ServerView.CAS:msg@231 messageId=
"screen.logout.header"][ServerView:audit@231 result=
"success"]Logout successful
```

STOP エントリ

次の STOP エントリには、構造化データに続けて要素 ServerView:audit@231 とフリーテキストが含まれています。

```
<110>1 2011-07-20T08:39:07.468+02:00 pontresina
ServerView.CAS - STOP
[ServerView:audit@231 result="success"]
[ServerView:msg@231 messageId"logging.syslog.operation.stop"]
Audit terminated
```

7 付録 1 - LDAP ディレクトリサービスによるグローバル iRMC S2/S3 ユーザ管理

iRMC S2/S3 によるユーザ管理には 2 種類の異なるユーザ ID を使用します。

– **ローカルユーザ ID** は iRMC S2/S3 内部の不揮発性記憶装置に保存され、iRMC S2/S3 のユーザインターフェース経由で管理されます。

– **グローバルユーザ ID** はディレクトリサービスの集中データストアに保存され、ディレクトリサービスのインターフェース経由で管理されます。

  グローバル iRMC S2/S3 ユーザ管理では、現在以下のディレクトリサービスがサポートされます。

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP[OpenLDAP]
  – OpenDS / OpenDJ

本章では以下について説明します。

– iRMC S2/S3 によるユーザ管理の概念
– ユーザ権限
– iRMC S2/S3 上のグローバルユーザ管理

i iRMC S2/S3 のローカルユーザ管理の詳細については、『iRMC S2/S3 - integrated Remote Management Controller』マニュアルを参照してください。

i ApacheDS では、iRMC S2/S3 の**電子メール設定**機能はサポートされません。

7.1 iRMC S2/S3 によるユーザ管理の概念

iRMC S2/S3 によるユーザ管理は、ローカルとグローバルのユーザ ID を並列に管理することができます。

ユーザがいずれかの iRMC S2/S3 のインターフェースにログインするために入力する認証データ（ユーザ名、パスワード）を検証する際には、iRMC S2/S3 は以下のように処理します（合わせて 141 ページ の図 39 も参照してください）。

1. iRMC S2/S3 はユーザ名とパスワードを内部に保存されたユーザ ID と照合します。
   - ユーザは、iRMC S2/S3 認証に成功すれば（ユーザ名とパスワードが有効）ログインすることができます。
   - 認証に失敗した場合には、iRMC S2/S3 はステップ 2 の検証手順を継続します。
2. iRMC S2/S3 はユーザ名とパスワードを使用して、LDAP 経由でディレクトリサービスの認証を受け、LDAP クエリによってユーザの権限を判断してユーザに iRMC S2/S3 を操作する権限があるかどうかを確認します。

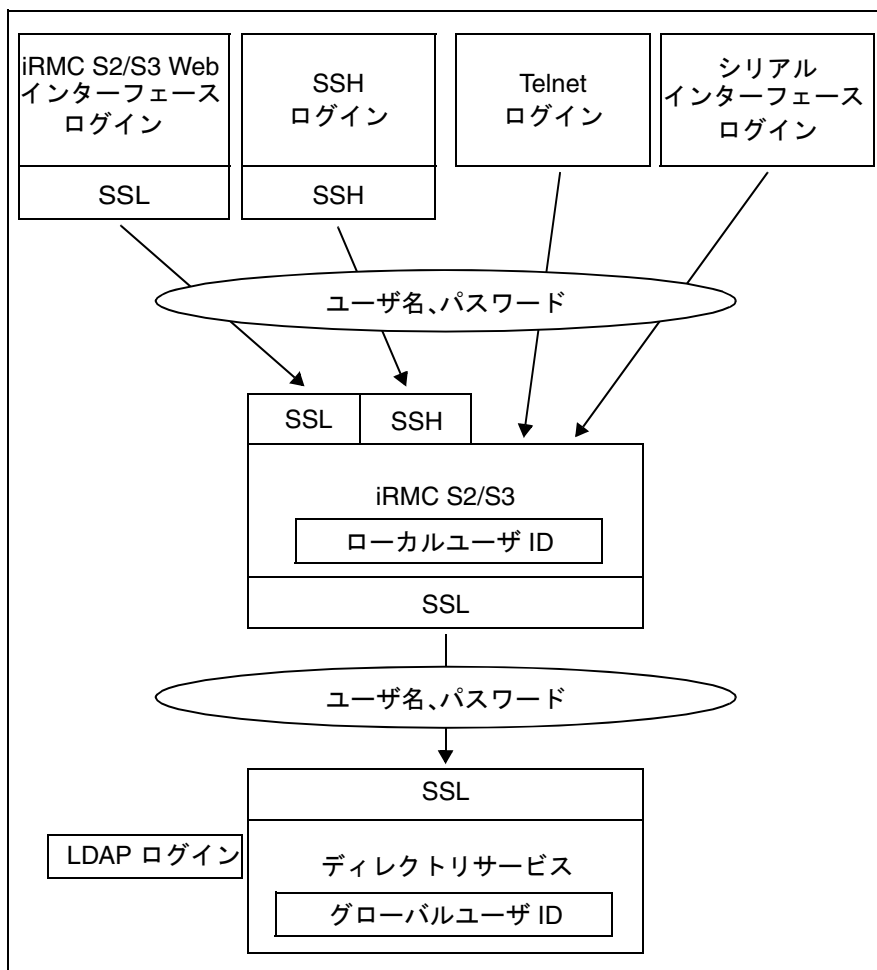



図 39: iRMC S2/S3 経由のログイン認証

iRMC S2/S3 とディレクトリサービスの間の LDAP 接続には、オプションの SSL を使用することを推奨します。SSL で保護された iRMC S2/S3 とディレクトリサービスの間の LDAP 接続では安全なデータ交換が保証されますが、特にユーザ名とパスワードのデータの送信が安全にできます。

iRMC S2/S3 Web インターフェース経由の SSL ログインが必要になるのは、LDAP が有効な場合のみです（「**LDAP 有効化**」オプション、『iRMC S2/S3 - integrated Remote Management Controller』マニュアルを参照）。

7.2 iRMC S2/S3 のグローバルユーザ管理

iRMC S2/S3 のグローバルユーザ ID は、LDAP ディレクトリサービスを利用して集中管理されます。

iRMC S2/S3 ユーザ管理では、現在以下のディレクトリサービスがサポートされます。

– Microsoft® Active Directory
– Novell® eDirectory
– OpenLDAP[OpenLDAP]
– OpenDS / ForgeRock's OpenDJ !!!

この節では次の点について説明します。

– iRMC S2/S3 のグローバルユーザ管理の概略

– LDAP ディレクトリサービスによる iRMC S2/S3 のグローバルユーザ管理の概念

– ディレクトリサービスによるグローバル iRMC S2/S3 ユーザ管理の設定（ディレクトリサービス中で iRMC S2/S3 に特化した許可構造の生成）

– Microsoft Active Directory によるグローバル iRMC S2/S3 ユーザ管理

– Global iRMC S2/S3 によるグローバル iRMC S2/S3 ユーザ管理

– OpenLDAP / OpenDS / OpenDJ!!! によるグローバル iRMC S2/S3 ユーザ管理

i 本節で説明される、ディレクトリサービスのためにユーザが実行する作業とは別に、グローバルユーザ管理には、iRMC S2/S3 上でローカルの LDAP 設定を設定する必要があります。

以下のいずれかの？法でローカル LDAP を設定します。

– iRMC S2/S3 Web インターフェース（『iRMC S2/S3 - integrated Remote Management Controller』マニュアルを参照）

– Server Configuration Manager の使用

i **なお、次の点に注意してください。**

グローバル iRMC S2/S3 ユーザ管理の設定を行うには、使用するディレクトリサービスに関して熟知している必要があります。ディレクトリサービスを熟知した管理者以外は作業を行わないでください。

7.2.1 「概要」

iRMC S2/S3 のグローバルユーザ ID は、ディレクトリサービスのディレクトリにすべてのプラットフォームの分が集中保管されています。これにより、集中サーバによるユーザ ID 管理が可能となっています。そのため、ネットワークでこのサーバに接続されているすべての iRMC S2/S3 で、ユーザ ID を使用することができます。

そのうえ、iRMC S2/S3 のディレクトリサービスを使用することにより、管理対象サーバのオペレーティングシステムに使用されるものと同じユーザ ID を iRMC S2/S3 へのログインにも使用することが可能です。

i グローバルユーザ管理は現在 iRMC S2/S3 の以下の機能ではサポートされていません。

– IPMI-over-LAN 経由のログイン
– SOL 経由のコンソールリダイレクション

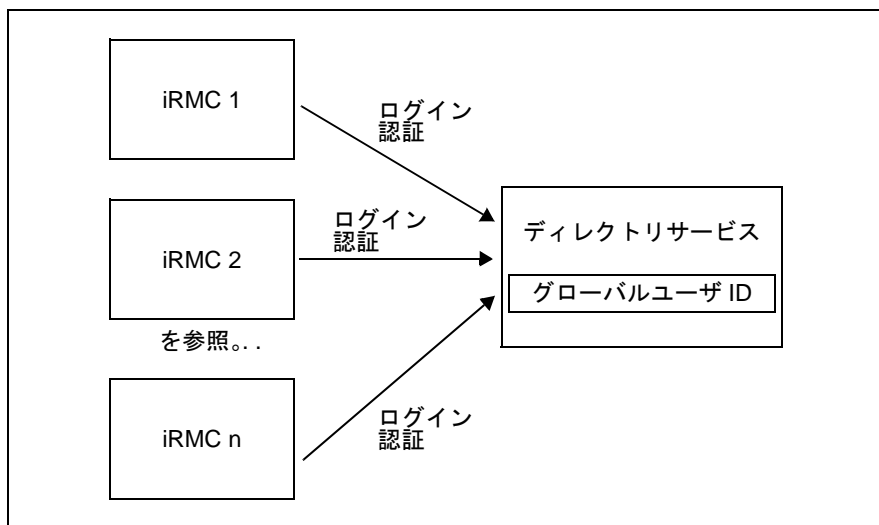



図 40: 複数の iRMC によるグローバルユーザ ID の共用

個々の iRMC S2/S3 と集中ディレクトリサービスの間の通信は TCP/IP プロトコル LDAP （**L**ightweight **D**irectory **A**ccess **P**rotocol）経由で実行されます。LDAP によって、ディレクトリサービスにアクセスする方法が最もよく使われ、ユーザ管理に最も適しています。オプションで、LDAP 経由の通信は、SSL によってセキュリティを確保することができます。

7.2.2 LDAP ディレクトリサービスによるグローバル iRMC S2/S3 ユーザの管理 （概念）

i 以下に説明するディレクトリサービスに基づくグローバル iRMC S2/S3 ユーザ管理の概念は、Microsoft Active Directory、Novell eDirectory、OpenLDAP および OpenDS / OpenDJ にも同様に適用されます。図は、Microsoft Active Directory のユーザインターフェースの「**Active Directory ユーザとコンピュータ**」コンソールの例に基づいています。

i 以下の記号は、LDAP 上で文字列を検索するためのメタキャラクタとして予約されています : *, \, &, (,), |, !, =, <, >, ~, :

したがって、ユーザはこれらの文字を相対識別名（RDN）の要素として使用することはできません。

7.2.2.1 役割を使用するグローバル iRMC S2/S3 ユーザ管理

LDAP ディレクトリサーバ経由のグローバル iRMC S2/S3 ユーザ管理では、標準のディレクトリサーバのスキーマを拡張する必要はありません。その代わりに、ディレクトリサーバに関連するすべての情報は、ユーザ権限も含めて、追加 LDAP グループと組織単位（OU）を使用して提供されます。これらの OU は、LDAP ディレクトリサーバのドメイン内の別々の OU で結合されたものです（147 ページ の図 42 を参照）。

iRMC S2/S3 ユーザは、組織単位（OU）**SVS** で宣言された役割（ユーザ役割）を割り当てられることで、権限を取得します。

ユーザロール（略称 : ロール）による許可の割り当て

iRMC S2/S3（ファームウェアバージョン 3.77 以降）のグローバルユーザ管理では、許可の割り当てをユーザロールにより管理します。この場合は、各ロールは、iRMC S2/S3 上で有効なタスクに基づく許可プロファイルを個々に定義します。

各々のユーザには複数のロールを割り当てることができますので、そのユーザの許可は、割り当てられたロールすべての許可の合計により定義されます。

図 41 は、**Administrator**、**Maintenance**、**Observer** および **UserKVM** の各ロールによるユーザ権限の、ロールに基づく割り当ての概念を図解したものです。

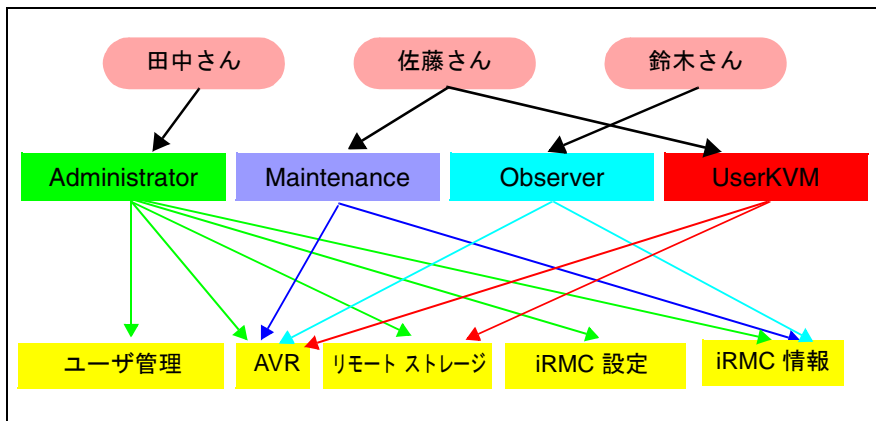



図 41: ロールに基づくユーザ権限の割り当て

ユーザロールの概念には、以下のような重要な利点があります。

– 各々のユーザまたはユーザグループに、個別に許可を割り当てる必要がない。その代わりに、許可はユーザロールに従って割り当てられる。

– 許可のストラクチャが変更になった場合にユーザロールによる許可を適合させるのみでよい。

7.2.2.2 組織単位（OU）SVS

iRMC S2 のファームウェアバージョン 3.77A および iRMC S3 は、OU **SVS** に保存されている LDAP v2 構造をサポートします。LDAP v2 構造はすべて今後の機能拡張のために設定されています。

i 追加の OU（**iRMCgroups**）が互換性の理由でサポートされ、iRMC S2（ファームウェアバージョン 3.77 以下を使用）および iRMC でもグローバルユーザ管理を実行できます。詳細については、マニュアルを参照してください。

– 『iRMC S2/S3 - integrated Remote Management Controller』、2011 年 5 月以前の版

– 「iRMC - integrated Remote Management Controller」。

「**SVS**」には、OU「**Declarations**」、「**Departments**」および「**User Settings**」が含まれています。

– 「**Declarations**」には、定義されたロールのリストと定義済みの iRMC S2/S3 ユーザ権限のリストが含まれています。

– 「**Departments**」にはユーザ権限のためのグループが含まれています。

– 「**User Settings**」には、メールフォーマット（警告メールに使用します）などのユーザまたはユーザグループ固有の詳細情報と、ユーザシェルのためのグループが含まれています。

i たとえば、Microsoft Active Directory の場合には、iRMC S2/S3 ユーザのエントリは標準 OU である「**Users**」に納められています。ただし、iRMC S2/S3 ユーザは標準ユーザとは異なり、OU「**SVS**」の 1 つまたは複数のグループのメンバーにもなっています。

i **注意事項 :**

ServerView ユーザ管理と iRMC S2/S3 グローバルユーザ管理の両方を同じ組織単位（OU）**SVS** で動作させるには、iRMC S2/S3 ユーザ管理が **DEFAULT** 部門に属するように設定する必要があります。

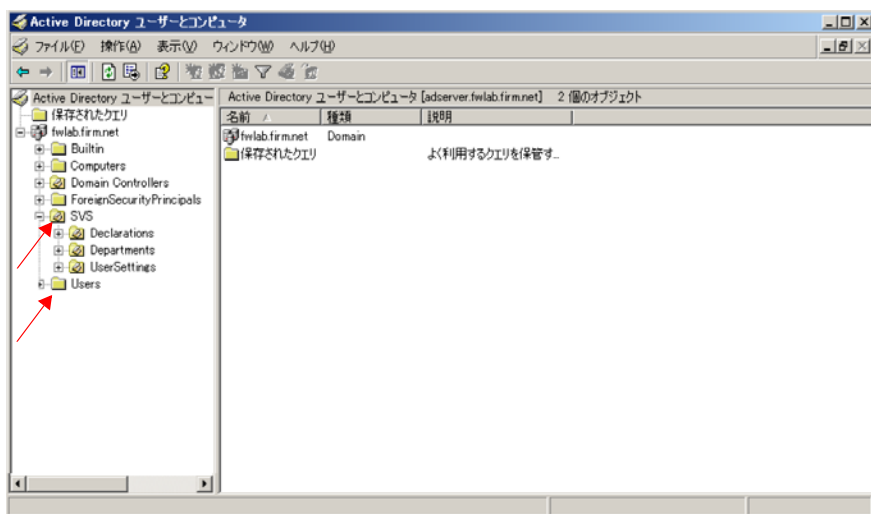



図 42: ドメイン fwlab.firm.net での OU SVS

バージョン 3.6x のファームウェアでは、iRMC S2/S3 用のユーザエントリは基本ドメインの配下のどのポイントにも配置できます。許可グループも基本ドメインの配下のどのポイントにも配置できます。

7.2.2.3　多部門サーバからのアクセス許可

大規模な企業では、iRMC S2/S3 によって管理されるサーバ群は通常さまざまな部門に割り当てられます。その上、管理対象サーバの管理者権限も、多くの場合部門独自の方法で割り当てられます。

注意事項：

ServerView ユーザ管理と iRMC S2/S3 グローバルユーザ管理の両方を同じ組織単位（OU）**SVS** で動作させるには、iRMC S2/S3 ユーザ管理が **DEFAULT** 部門に属するように設定する必要があります。

部門は「Departments」という OU 内で結合されます

OU「**Departments**」は、iRMC S2/S3 によって管理されるサーバを結合し、多数のグループを形成します。これらは、同じユーザ ID と許可が適用される部門に対応します。たとえば、149 ページ の図 43 では、「**DeptX**」、「**DeptY**」および「**Others**」という部門になります。

「**Others**」というエントリは任意ですが推奨します。「**Others**」は、どの部門にも属さないすべてのサーバを含む、あらかじめ定義された部門名です。「**Departments**」の下にリストされる部門（OU）の数に関しては、制限はありません。

iRMC S2/S3 でディレクトリサービスを iRMC S2/S3 Web インターフェース（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』を参照）、または Server Configuration Manager を使用して直接サービスを設定する場合は、関連する iRMC S2/S3 が属する管理対象サーバの部門名を指定します。LDAP ディレクトリにその名前の部門がない場合には、「**Others**」部門にある権限を使用します。

149 ページ の図 43 は、**Active Directory ユーザとコンピュータ**を基本としたこのタイプの組織構造の例を表します。

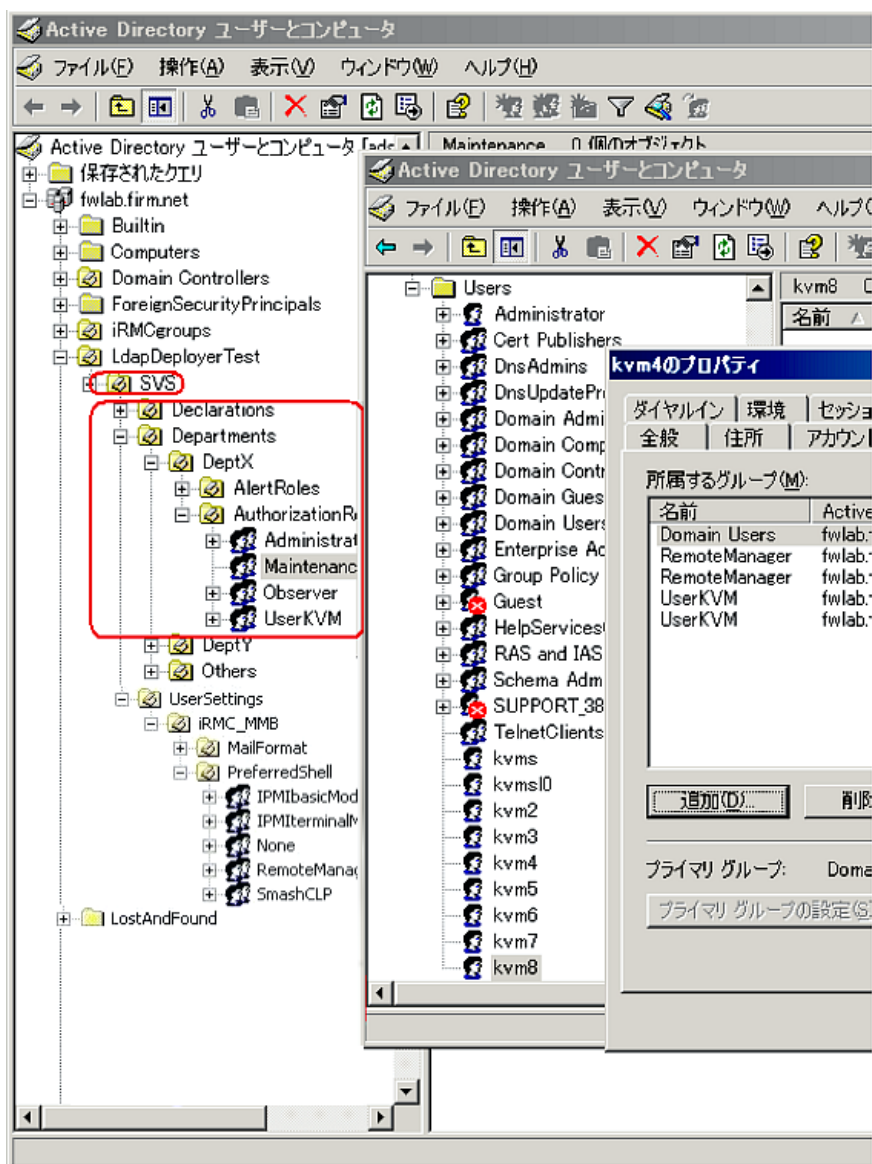



図 43: ドメイン fwlab.firm.net の組織構造

7.2.2.4 SVS: 許可プロファイルはロールにより定義される

要求される関連ユーザロール（認証ロール）は各部門の直下にリストされます（149 ページ の図 43）。ここにリストされるロールはすべて OU「**Declarations**」で定義されます。それ以外にロールの数に関する制限はありません。ロールの名前は必要に応じて選ぶことができますが、運用するディレクトリサービスに賦課された特定のシンタックス要件に合わなければなりません。各認証ロールは、iRMC S2/S3 上の処理のためにタスクに基づく許可プロファイルを個々に定義します。

> **i** 認証ロールと同様に警告ロールもリストされます。各警告ロールには Email で警告するための固有の警告プロファイルを定義します（208 ページ の「グローバル iRMC S2/S3 ユーザ宛ての Email 警告の設定」の項を参照）。

ユーザロールの表示

「**Active Directory ユーザとコンピュータ**」のストラクチャツリー（図 44 を参照）の「**SVS**」の配下にある部門（たとえば **DeptX**）を選択し（1）、関連するノード「**DeptX – Authorization Roles**」を展開すると、そこに定義されたユーザ役割（ここでは **DeptX**）が表示されます（2）。

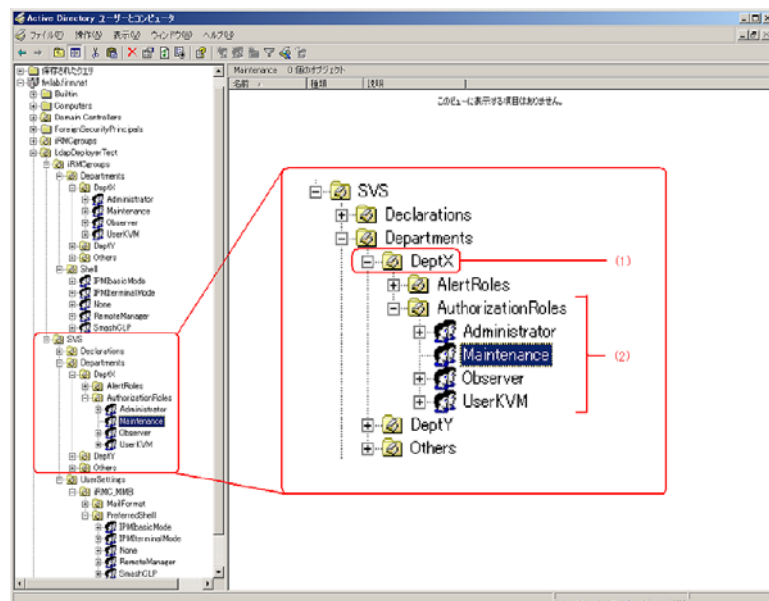



図 44: 「ユーザとコンピュータ」スナップインの中のユーザロールの表示

ユーザがメンバーとなっている Active Directory フォルダの表示

「**Active Directory ユーザとコンピュータ**」のストラクチャツリーの「**Users**」の配下にあるユーザ（**kvms4** など）を選択して（図 45 を参照）(1)、コンテキストメニューから「**プロパティ**」-「**所属するグループ**」を選択してこのユーザの「**プロパティ**」ダイアログボックスを開いた場合、ユーザが属する権限グループ（ここでは **kvms4**）が「**所属するグループ**」タブに表示されます (2)。

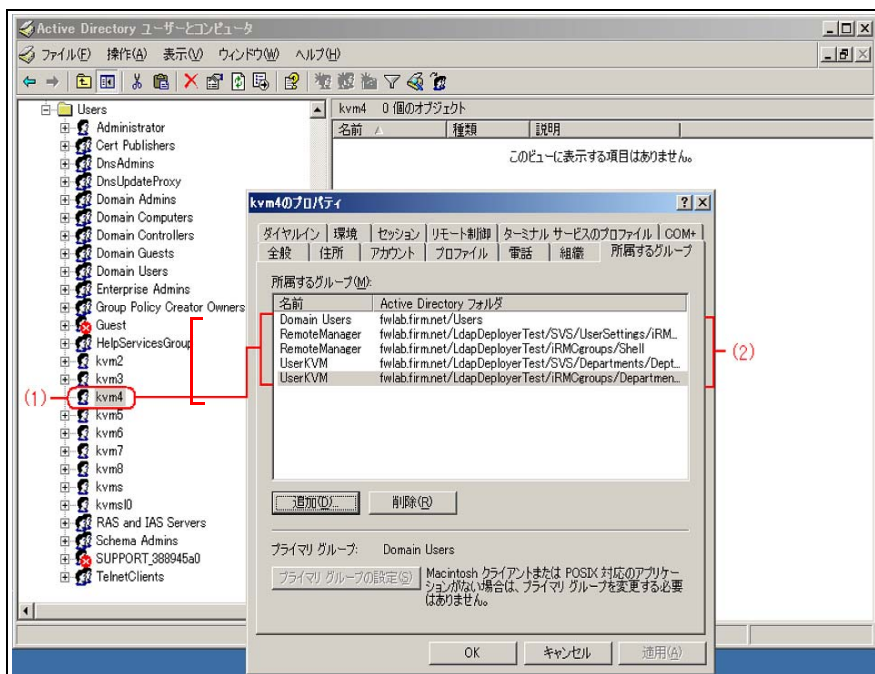



図 45: ユーザ「kvms4」のプロパティダイアログボックス

7.2.3 SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除

ディレクトリサービスを使用してグローバル iRMC S2/S3 ユーザ管理を操作できるようにするために、LDAP ディレクトリに「**SVS**」ストラクチャ（OU）を作成する必要があります。

「**SVS**」ストラクチャの生成または変更には **SVS_LdapDeployer** を使用します。「**SVS_LdapDeployer**」は Java アーカイブ（「**SVS_LdapDeployer.jar**」）ですが、ServerView Suite の DVD に収録されています。

この節では以下について説明します。

– 「**SVS_LdapDeployer**」の設定ファイル
– **SVS_LdapDeployer**
– 「**SVS_LdapDeployer**」のコマンドとオプション
– 一般的な使用例

7.2.3.1 設定ファイル（XML file）

「**SVS_LdapDeployer**」は **XML** 設定ファイルに基づいて LDAP ストラクチャを生成します。この入力ファイルには、ストラクチャ「**SVS**」の XML 構文によるストラクチャ情報が含まれています。

i 設定ファイルの構文については、サンプル設定ファイル「**Generic_Settings.xml**」および「**Generic_InitialDeploy.xml** 」で説明されています。これらのファイルは、ServerView Suite DVD に収録される **jar** アーカイブ「**SVS_LdapDeployer.jar** 」の中にあります。

i ディレクトリサーバ接続のための有効な接続データはかならず <Settings> 入力ファイルの下に入力しなければなりません。

サーバにアクセスするための認証データは任意で入力することができます。あるいは、「**SVS_LdapDeloyer**」のコマンドラインで認証データを指定することもできます。

「**SVS_LdapDeployer**」を呼び出すときに設定ファイルまたはコマンドラインで認証データを指定しないと、「**SVS_LdapDeployer**」から認証データをランタイムで入力するように求められます。

7.2.3.2 SVS_LdapDeployer の起動

以下の手順に従って、**SVS_LdapDeployer** を起動します。

► Java アーカイブ（**jar** アーカイブ）の「**SVS_LdapDeployer.jar**」をディレクトリサーバ上のフォルダに保存します。

► ディレクトリサーバのコマンドインターフェースを開きます。

► **jar** アーカイブ「**SVS_LdapDeployer.jar**」が保存されているフォルダに移動します。

► 次の構文を使用して「**SVS_LdapDeployer**」を呼び出します。

```
java -jar SVS_LdapDeployer.jar <command> <file>
                                              [<option>...]
```

i 「**SVS_LdapDeployer**」の実行中に行われるさまざまな手順が通知されます。詳細な情報は **log.txt** ファイルで見ることができます。このファイルは「**SVS_LdapDeployer**」実行時に毎回実行フォルダの中に作られます。

i 以下では、「LDAPv1 ストラクチャ」と「LDAPv2 ストラクチャ」は、認証データの ServerView 固有の設定レイアウトを示すために使用され、LDAP プロトコルのバージョン 1 および 2 を指すものではありません。

i **-import** と **-sychronize** コマンド（以下を参照）は、LDAPv1 ストラクチャ（ファームウェアバージョン 3.77 未満搭載の iRMC S2 と iRMC）の場合にのみ必要です。詳細については、マニュアルを参照してください。

– 『iRMC S2/S3 - integrated Remote Management Controller』、2011 年 5 月以前の版

– 「iRMC - integrated Remote Management Controller」。

<command>

実行する処理を指定します。

以下のコマンドを使用可能です。

-deploy

グローバル iRMC S2/S3 ユーザ管理の LDAP ストラクチャをディレクトリサーバの中に作成します（155 ページを参照）。

-delete

グローバル iRMC S2/S3 ユーザ管理に用いた LDAP ストラクチャをディレクトリサーバから削除します（157 ページを参照）。

-import

既存の LDAP v1 ストラクチャから 同等の LDAP v2 ストラクチャを作成します。

-synchronize

LDAP v2 に何らかの変更を行うと、その変更を反映して既存の LDAP v1 ストラクチャを同じように変更します。

<file>

「**SVS_LdapDeploy**」が入力ファイルとして用いる設定ファイル（**.xml**）。この設定ファイルには、**SVS** ストラクチャのストラクチャ情報が **XML** 構文で含まれています。

> i 設定ファイルの構文については、サンプル設定ファイル「**Generic_Settings.xml**」および「**Generic_InitialDeploy.xml** 」で説明されています。これらのファイルは、ServerView Suite DVD に収録される **jar** アーカイブ「**SVS_LdapDeployer.jar** 」の中にあります。

<option> [<option> ...]

指定されたコマンドの実行をコントロールするためのオプションです。

これ以降の項では、「**SVS_LdapDeployer**」で使用できる個々のコマンドを関連するオプションと合わせて詳しく解説します。

> i 「**SVS_LdapDeployer**」は、すべてのグループが含まれる必要なサブツリーを生成しますが、ユーザとグループの関連付けはしません。
>
> ユーザエントリは、ディレクトリサービスで OU「**SVS**」か「iRMCgroups」または双方を生成した後、運用するディレクトリサービスの適切なツールを使用して作成し、グループに割り当てます。

7.2.3.3 -deploy: LDAP v2 ストラクチャの作成と変更

-deploy コマンドを使用して、ディレクトリサーバ上に新しい LDAP ストラクチャを作成したり、既存の LDAP ストラクチャに新しいエントリを追加したりすることができます。

既存の LDAP ストラクチャからエントリを削除する場合は、まず **-delete** コマンド（157 ページを参照）を使用して LDAP ストラクチャ自体を削除し、次に適切に修正した設定ファイルを使用して LDAP ストラクチャを再作成する必要があります。

構文：

```
-deploy <file> [-structure {v1 | v2 | both}]
      [ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

設定データを含む **XML** ファイル。

設定ファイルの <Data> 部にはストラクチャを最初に生成するため、または展開するために必要なロールと部門がすべて含まれなければなりません。

-structure v1 **|** -structure v2 **|** -structure both

LDAP v1 ストラクチャまたは、LDAP v2 ストラクチャ、あるいは、LDAP v1 と LDAP v2 両方のストラクチャを作成します。

ファームウェアバージョン 3.77A の iRMC S2 と iRMC S3 のユーザ管理では、常に LDAP v2 ストラクチャが必要です。

-username <user>

ディレクトリサーバにログインするためのユーザ名です。

-password <password>

ユーザ <user> のパスワード。

-store_pwd

-deploy が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルトでは、ランダムに生成された鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保存してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザもアクセスできる場合は、オプション **-kloc** および **-kpwd** を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。
<password> が指定されない場合は、現行のランタイムのスナップショットを基にしてパスワードが自動的に生成されます。

7.2.3.4 -delete: LDAP v2 ストラクチャの削除

-delete コマンドを使用して、ディレクトリサーバから LDAP v2 ストラクチャを削除することができます。

構文：

```
-delete <file> [-structure {v1 | v2 | both}]
      [ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

削除するストラクチャを指定する **XML** ファイルです。

-structure v1 **|** -structure v2 **|** -structure both

LDAP v1 ストラクチャまたは、LDAP v2 ストラクチャ、あるいは、LDAP v1 と LDAP v2 両方のストラクチャを削除します。

ファームウェアバージョン 3.77A の iRMC S2 と iRMC S3 のユーザ管理では、常に LDAP v2 ストラクチャが必要です。

-username <user>

ディレクトリサーバにログインするためのユーザ名です。

-password <password>

ユーザ <user> のパスワード。

-stor_pwd

-delete が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルトでは、ランダムに生成された鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保存してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザもアクセスできる場合は、オプション **kloc** および **-kpwd** を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。<password> が指定されない場合は、現行のランタイムのスナップショットを基にしてパスワードが自動的に生成されます。

7.2.4 一般的な使用例

「**SVS_LdapDeployer**」を使用する際の一般的な使用例を、以下に示します。

7.2.4.1 LDAP v2 ストラクチャの初期設定の実行

iRMC S2/S3（ファームウェア 3.77 以降）のグローバルユーザ管理を初めて設定する場合、LDAP v2 のストラクチャが必要となります。

推奨する方法：

LDAP v2 ストラクチャの部門定義を生成します（**SVS**）。

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure v2
```

7.2.4.2 LDAP v2 ストラクチャの再生成と展開

LDAP v2 ストラクチャを再生成するか、既存の LDAP v2 ストラクチャを展開したい場合。

推奨する方法：

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure -structure v2
```

または

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
```

7.2.4.3 LDAP v2 ストラクチャの再生成と、認証データの要求と保存

LDAP v2 ストラクチャを再生成したい場合。認証データはコマンドラインを用いて作成し、保存します。

推奨する方法：

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -store_pwd -username admin -password admin
```

ℹ ログインデータを保存した後には、ユーザ名およびパスワードを指定せずに「**SVS_LdapDeployer**」を使用してディレクトリサーバに接続できます。その際、使用可能な数値が XML 設定ファイルに保存されている場合は、「**SVS_LdapDeployer**」はその数値を使用します。
「**SVS_LdapDeployer**」が保存されたパスワードを使用できるのは、暗号化されたパスワードを解読できる場合のみです。そのため、「**SVS_LdapDeployer**」を、「**-store_pwd**」オプション（156 ページを参照）を用いた前の呼び出しで適用したのと同じランタイム環境で実行する必要があります。このコンテキストで言う「同じランタイム環境」とは、「同じコンピュータを使用する同じユーザ」または「鍵が保存されているフォルダにアクセスする許可を持つユーザ（**-kloc** オプション、156 ページを参照）」を意味します。

ℹ 今後は、「**SVS_LdapDeployer**」を呼び出すときに、すでに保存してあるユーザアカウントを使用することもできます。さらに、データをコマンドラインに明確に指定するか、「**SVS_LdapDeployer**」がそのように要求する場合には、他の認証データを一時的に使用することもできます。

7.2.5 Microsoft Active Directory による iRMC S2/S3 ユーザ管理

この項では、iRMC S2/S3 ユーザ管理を Microsoft Active Directory に統合する方法を説明します。

前提条件：

LDAP v2 ストラクチャまたはそのいずれかが Active Directory サービスの中に生成されていること（152 ページ の「SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除」の項を参照）。

以下の手順を実行して、iRMC S2/S3 ユーザ管理を Microsoft Active Directory に統合します。

1. Active Directory サーバ上の iRMC S2/S3 LDAP/SSL アクセスを設定します。
2. iRMC S2/S3 のユーザを Active Directory の iRMC S2/S3 ユーザグループに割り当てます。

7.2.5.1 Active Directory サーバ上の iRMC S2/S3 LDAP/SSL アクセスの設定

iRMC S2/S3-LDAP の統合には、OpenSSL プロジェクトに基づき Eric Young 氏が開発した SSL 実装を使用します。SSL copyright の複製リストを 216 ページ に掲載します。

iRMC S2/S3 が SSL 経由で LDAP を使用できるようにするには、RSA 証明書が必要です。

LDAP アクセスを設定する手順は以下の通りです。

1. 企業 CA をインストールします。
2. ドメインコントローラ用の RSA 証明書を生成します。
3. RSA 証明書をサーバにインストールします。

企業 CA のインストール

CA は「認証局」です。企業 CA（認証局）はドメインコントローラ自体または別のサーバにインストールすることができます。

ディレクトリサーバをドメインコントローラに直接インストールするほうが、別のサーバにインストールするよりも必要な手順が少ないので簡単です。

企業 CA をドメインコントローラ以外のサーバにインストールする方法を、以下に説明します。

企業 CA をインストールして正しく設定するには、Active Directory 環境とインストール済みの IIS（**I**nternet **I**nformation **S**ervices）が必要です。

企業 CA のインストールは以下の手順で行います。

▶ Windows のスタートメニューで、次のように進みます。

「スタート」-「コントロールパネル」-「プログラムの追加と削除」-「Windows コンポーネントの追加と削除」

▶ Windows コンポーネントのウィザードで、「**Components**」から「**Certificate Services**」を選択します。

▶ 「**Certificate Services**」をダブルクリックし、「**Certificate Services Web Enrollment Support**」と「**Certificate Services CA**」のオプションが選択されていることを確認します。

▶ 「**Enterprise root CA**」を選択します。

- オプション「**Use custom settings to generate the key pair and CA certificate**」を選択します。
- 「**Microsoft Base DSS Cryptographic Provider**」を選択して長さ 1024 バイトの DSA 証明書を作成します。
- 公開認証局証明書（CA 証明書）をエクスポートします。

  これは次の手順で行います。

  - Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させます。
  - ローカルコンピュータ証明書のスナップインを追加します。
  - **「Certificates（Local Computer）」-「Trusted Root Certification Authorities」-「Certificates」**へと進み、ダブルクリックします。
  - 新規に作成された認証局からの証明書をダブルクリックします。
  - 証明書ウィンドウの「**Details**」タブをクリックします。
  - 「**Copy to File**」をクリックします。
  - 認証局証明書のファイル名を選び、「**Finish**」をクリックします。
- 公開認証局証明書をドメインコントローラ上の証明書ディレクトリ **Trusted Root Certification Authorities** にロードします。

  これは次の手順で行います。

  - 認証局証明書を収めたファイルをドメインコントローラに転送します。
  - Windows エクスプローラーで、新規に作成された認証局からの証明書を開きます。
  - 「**Install Certificate**」をクリックします。
  - 「**Place all certificates in the following store**」の下の「**Browse**」をクリックし、「**Trusted Root Certification Authorities**」を選択します。
  - Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させます。
  - ローカルコンピュータ証明書のスナップインを追加します。
  - 現在のユーザの証明書のスナップインを追加します。
  - 認証局証明書（CA 証明書）を、現在のユーザの **Trusted Root Certification Authorities** ディレクトリからローカルコンピュータの **Trusted Root Certification Authorities** にコピーします。

ドメインコントローラ証明書の作成

ドメインコントローラの RSA 証明書の作成は、以下の手順で行います。

▶ 下記の内容の **request.inf** という名前のファイルを作成します。

```
[Version]
Signature="$Windows NT$"[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

RequestType = PKCS10
OID=1.3.6.1.5.5.7.3.1
; サーバ認証用
```

▶ ファイル **request.inf** で、「Subject=」の下の指定を、用いているドメインコントローラの名前に合わせます（例 :
`Subject = “CN=domino.fwlab.firm.net”`。

▶ Windows のプロンプトウィンドウに、「**certreq -new request.inf request.req**」と入力します。

▶ 認証局ブラウザに次の URL を入力します :
http://localhost/certsrv

▶「**Request a Certificate**」をクリックします。

▶「**advanced certificate request**」をクリックします。

▶「**Submit a certificate request**」をクリックします。

▶ ファイル **request.req** の内容を「**Saved Request**」ウィンドウにコピーします。

▶「**Web Server**」証明書のテンプレートを選択します。

▶ 証明書をダウンロードして、ファイル **request.cer** などに保存します。

► Windows のプロンプトウィンドウに、「**certreq -accept request.cer**」と入力します。

► 証明書を秘密鍵付きでエクスポートします。

これは次の手順で行います。

- ► Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させます。
- ► ローカルコンピュータ証明書のスナップインを追加します。
- ► 以下の順に移動します。
  「Certificates（Local Computer）」- 「Personal Certificates」- 「Certificates」
- ► 新規サーバ認証局証明書をクリックします。
- ► 証明書ウィンドウの「**Details**」タブをクリックします。
- ► 「**Copy to File**」をクリックします。
- ► 「**Yes, export the private key**」を選択します。
- ► パスワードを割り当てます。
- ► 証明書のファイル名を選び、「**Finish**」をクリックします。

ドメインコントローラ証明書のサーバへのインストール

ドメインコントローラ証明書のサーバへのインストールは、次の手順で行います。

- ► 作成されたばかりのドメインコントローラ証明書のファイルをドメインコントローラにコピーします。
- ► ドメインコントローラ証明書をダブルクリックします。
- ► 「**Install Certificate**」をクリックします。
- ► 証明書をエクスポートするときに割り当てたパスワードを使用します。
- ► 「**Place all certificates in the following store**」の下の「**Browse**」をクリックし、「**Personal Certificates**」を選択します。
- ► Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させます。
- ► ローカルコンピュータ証明書のスナップインを追加します。
- ► 現在のユーザの証明書のスナップインを追加します。
- ► ドメインコントローラ証明書を現在のユーザの **Personal Certificates** ディレクトリからローカルコンピュータの **Personal Certificates** ディレクトリにコピーします。

7.2.5.2 iRMC S2/S3 ユーザへのユーザロールの割り当て

iRMC S2/S3 ユーザにユーザロール（認証ロール）を以下の方法で割り当てることができます。

– ユーザエントリに基づいて
– または、ロールエントリ / グループエントリ

i 以下の例では、LDAP v2 ストラクチャを使用して、OU「**SVS**」のロールエントリに基づく割り当てを説明しています。

ユーザエントリに基づく割り当て方法もほぼ同じです。

i Active Directory にユーザを手作業で入力する必要があります。

次の手順に従います。

► スナップイン「**Active Directory ユーザとコンピュータ**」を開きます。

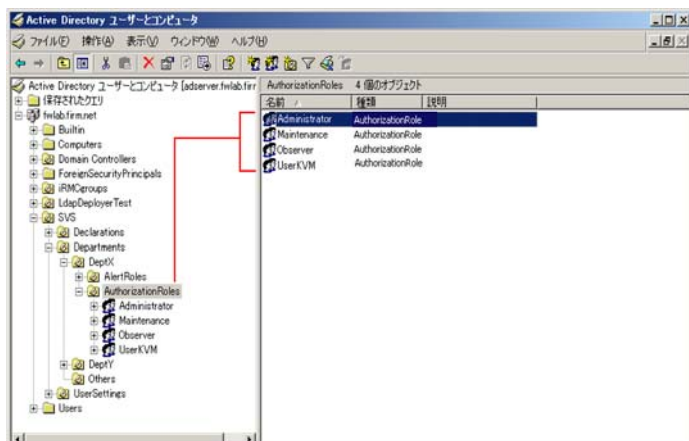



図 46: スナップイン「Active Directory ユーザとコンピュータ」

► 認証ロールをダブルクリックします（ここでは Administrator）。

「**Administrator のプロパティ**」ダイアログが開きます（167 ページ の図 47 を参照）。

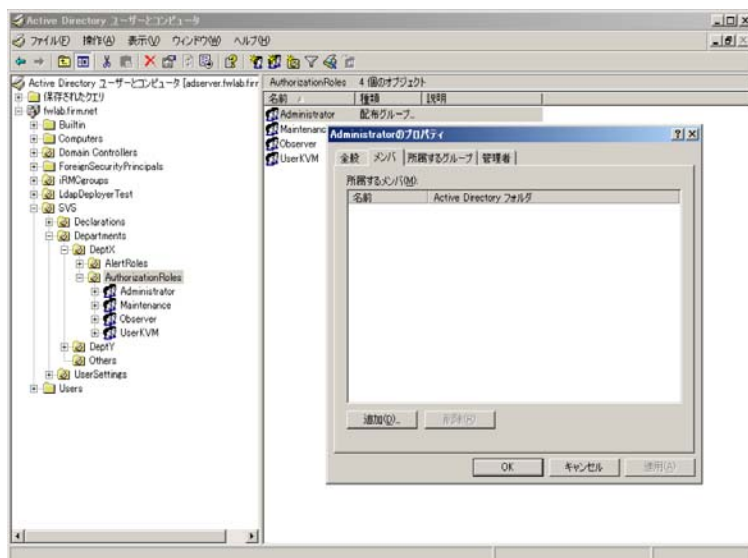



図 47: 「Administrator のプロパティ」ダイアログ

► 「**メンバ**」タブを選択します。

► 「**追加**」をクリックします。ボタンをクリックします。

「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログが開きます（167 ページ の図 48 を参照）。

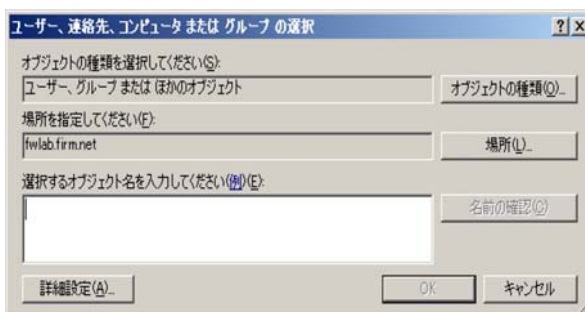



図 48: 「ユーザ、連絡先、コンピュータ または グループの選択」ダイアログ

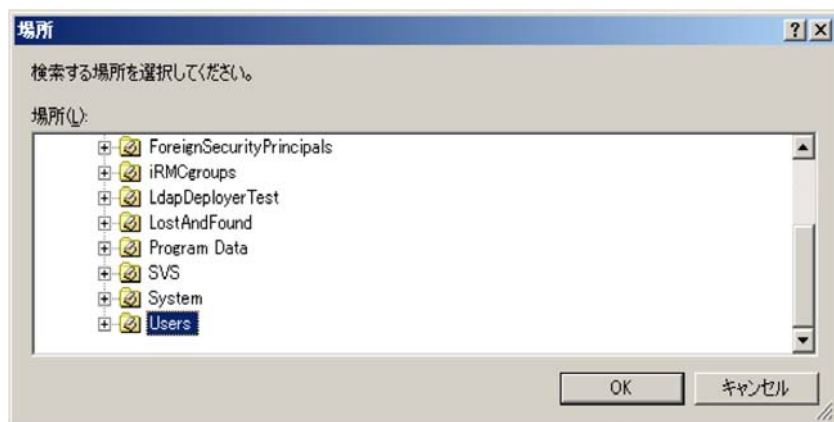
► 「**場所**」をクリックします。ボタンをクリックします。

「**場所**」ダイアログが開きます。

図 49: 「場所」ダイアログ

► 該当するユーザを含むコンテナ（OU）を選択します。（デフォルト値は OU「**Users**」となります）。「**OK**」をクリックして確定します。

「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログが開きます（168 ページ の図 50 を参照）。

i ディレクトリ内の他の位置にユーザを ?? することもできます。

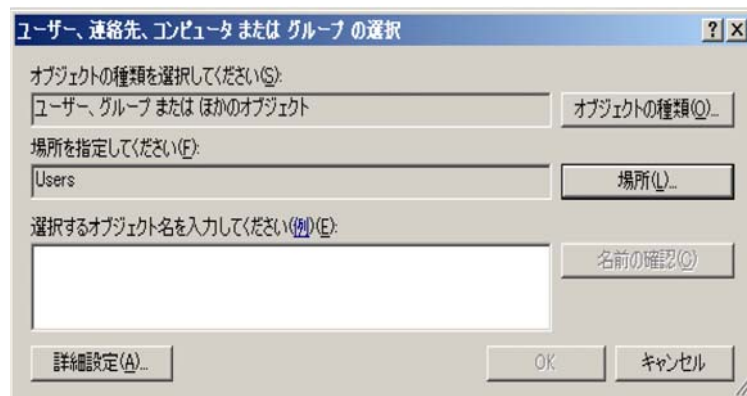



図 50: 「ユーザ、連絡先、コンピュータ または グループの選択」ダイアログ

► **「詳細設定」**をクリックします。ボタンをクリックします。

「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログが展開されます（169 ページ の図 51 を参照）。

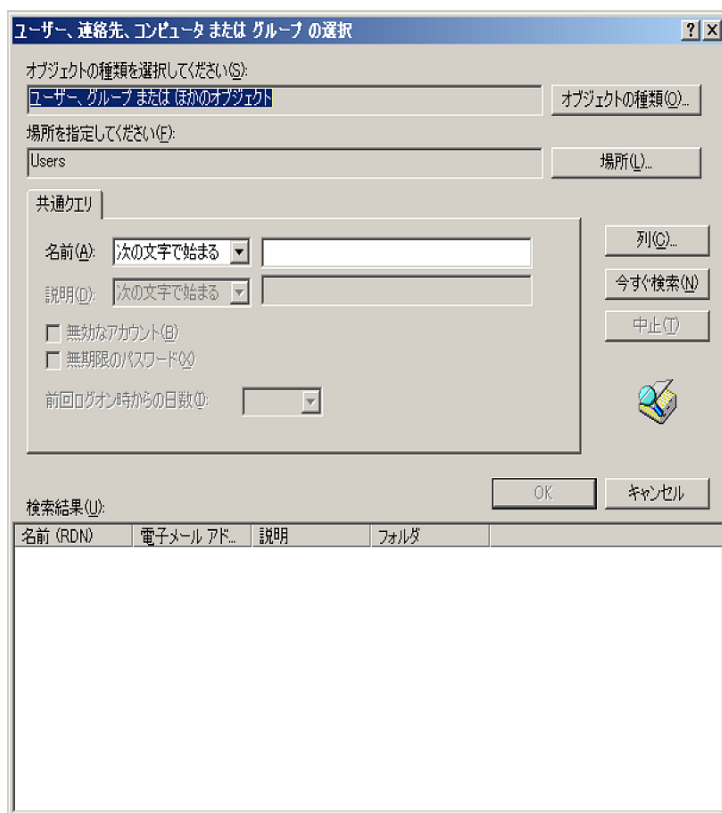



図 51: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ ? 検索画面

► 「**今すぐ検索**」ボタンをクリックしてドメイン内のすべてのユーザを表示させます。

「**検索結果**」の表示部に検索結果が表示されます（170 ページ の図 52 を参照）。

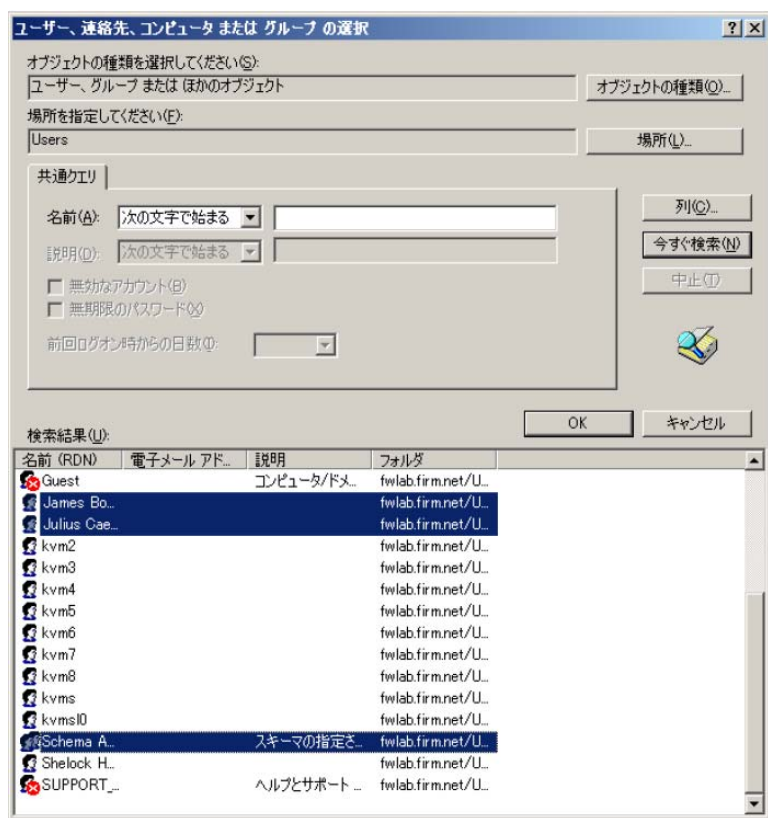



図 52: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ ? 検索結果表示

► グループに追加するユーザを選択し、「**OK**」をクリックして確定します。

選択したユーザが表示されます（171 ページ の図 53 を参照）。

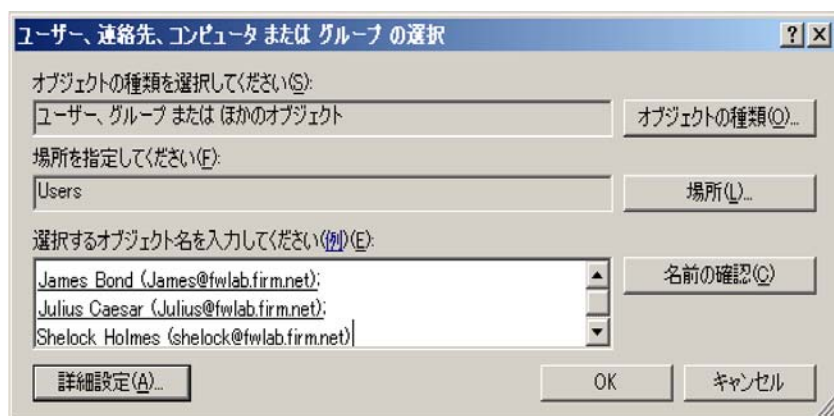



図 53: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ ? 検索結果確認

► 「**OK**」をクリックして確定します。

7.2.6 Novell eDirectory によるグローバル iRMC S2/S3 ユーザ管理

この節では次の点について説明します。

– Novell eDirectory システムのコンポーネントとシステム要件

– Novell eDirectory のインストール

– Novell eDirectory の設定

– iRMC S2/S3 ユーザ管理の Novell eDirectory への統合

– Novell eDirectory 管理のためのヒント

i 以下に Novell _eDirectory のインストールと設定を詳しく説明します。eDirectory についての広範な知識は必要ありません。すでに Novell eDirectory に習熟しているユーザは、初めの 3 つの節を飛ばして 186 ページ の「iRMC S2/S3 ユーザ管理の Novell eDirectory への統合」の項 に進んでください。

7.2.6.1 ソフトウェアコンポーネントとシステム要件

i 以下にリストされた指定されたバージョン以降のコンポーネントを使用してくださ い。

Novell eDirectory（以前の NDS）は次のソフトウェアコンポーネントで構成されています。

– eDirectory 8.8 : **20060526_0800_Linux_88-SP1_FINAL.tar.gz**

– eDirectory 8.8 : **eDir_88_iMan26_Plugins.npm**

– iManager: SuSE の場合は **iMan_26_linux_64.tgz**、それ以外は **iMan_26_linux_32.tgz**

– ConsoleOne : **c1_136f-linux.tar.gz**

Novell eDirectory をインストールし運用するには、以下のシステム要件を満たす必要があります。

– OpenSSL をインストールする必要があります。

  i OpenSSL がインストール済みでない場合、

  ► OpenSSL をインストール**してから**、Novell eDirectory のインストールを開始してください。

– 512 MB の RAM の空き領域

7.2.6.2 Novell eDirectory のインストール

Novell eDirectory をインストールするには、下記のコンポーネントをインストールする必要があります。

– eDirectory Server および管理ユーティリティ

– iManager（管理ユーティリティ）

– ConsoleOne（管理ユーティリティ）

Novell eDirectory インストールの前提条件 :

– Linux サーバ OS のフルインストールと稼動。

– ファイヤーウォールを次のポートに接続可能な設定にします :
8080, 8443, 9009, 81, 389, 636。

OpenSuSE では、ファイル **/etc/sysconfig/SuSEfirewall2** の中でこの設定を行います。

► ファイル **/etc/sysconfig/SuSEfirewall2** に、エントリ「**FW_SERVICES_EXT_TCP**」を次のように追加します。

```
FW_SERVICES_EXT_TCP="8080 8443 9009 81 389 636"
```

– eDirectory インストールガイドに従ってシステムにマルチキャストルーティングの設定を行います。

SuSE Linux の場合は以下の通り進めてください。

► ファイル **/etc/sysconfig/network/ifroute-eth0** を作成するか、（作成済みの場合は）開いてください。

► **/etc/sysconfig/network/ifroute-eth0** に以下の行を追加します。

```
224.0.0.0  0.0.0.0  240.0.0.0  eth0
```

この操作で *eth0* がシステム構成に取り込まれます。

eDirectory Server、eDirectory ユーティリティ、iManager および ConsoleOne インストールの前提条件 :

– インストールを実行するにはルート権限が必要です。

– 以下の手順でインストールを実行する前に、必要なすべてのファイルをディレクトリ（たとえば **/home/eDirectory**）にコピーしておく必要があります。必要なファイルは以下のとおりです。

20060526_0800_Linux_88-SP1_FINAL.tar.gz
iMan_26_linux_64.tgz
c1_136f-linux.tar.gz

eDirectory Server と管理ユーティリティのインストール

次の手順に従います。

► ルート権限（スーパーユーザ）でログインします。

► インストールに必要なファイルを含むディレクトリに移動します（この例では **/home/eDirectory**）。

```
cd /home/eDirectory
```

► **20060526_0800_Linux_88-SP1_FINAL.tar.gz** アーカイブを解凍します。

```
tar -xzvf 20060526_0800_Linux_88-SP1_FINAL.tar.gz
```

解凍すると、**/home/eDirectory** に **eDirectory** という新しいサブディレクトリが作られます。

eDirectory Server のインストール

► このディレクトリ **eDirectory** のサブディレクトリ **setup** に進みます。

```
cd eDirectory/setup
```

► インストール用スクリプト **./nds-install** を呼び出します。

```
./nds-install
```

► 「y」を入力して EULA を承認し、[Enter] キーで確定します。

► どのプログラムをインストールするか尋ねられたら、

「**install the Novell eDirectory server**」に「1」を入力し、[Enter] キーで確定します。

これで、eDirectory パッケージがインストールされます。

Novell eDirectory Server がインストールできたら、eDirectory までのパス名を環境変数で更新し、これらの変数をエクスポートします。

► この操作を行うには、設定ファイル（この例では「**/etc/bash.bashrc**」）を開き、次の行を指定された順序で「# End of ...」の前に入力します。

```
export PATH/opt/novell/eDirectory/bin:/opt/novell/eDirectory/
       sbin:$PATH

export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/
       opt/novell/eDirectory/lib/nds-modules:/opt/novell/
       lib:$LD_LIBRARY_PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
       man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
       locale:$TEXTDOMAINDIR
```

► ターミナルを閉じ、新しいターミナルを立ち上げて環境変数をエクスポートします。

eDirectory 管理ユーティリティのインストール

► ディレクトリ **eDirectory** のサブディレクトリ **setup** に移動します。

```
cd eDirectory/setup
```

► インストール用スクリプトを呼び出します。

```
./nds-install
```

► 「y」を入力して EULA を承認し、[Enter] キーで確定します。

► どのプログラムをインストールするか尋ねられたら、

「**install the Novell eDirectory adminsitration utilities**」に「2」を入力し、[Enter] キーで確定します。

これで、eDirectory 管理ユーティリティがインストールされます。

iManager のインストールと起動

> i Novell eDirectory のインストールには iManager を使用することを推奨します。SLES10 または OpenSuSE にインポートする場合は、アーカイブ ***_64.tgz** を使用します。

次の手順に従います。

- ルート権限（スーパーユーザ）でログインします。
- ディレクトリ **/home/eDirectory** に移動します。

```
cd /home/eDirectory
```

- アーカイブ **iMan_26_linux_64.tgz** を解凍します。

```
tar -xzvf iMan_26_linux_64.tgz
```

解凍すると、**/home/eDirectory** に **iManager** という新しいサブディレクトリが作られます。

- **iManager** の **installs** サブディレクトリに進みます。

```
cd iManager/installs/linux
```

- インストール用スクリプトを呼び出します。

```
./iManagerInstallLinux.bin
```

- インストール時のメッセージを出力する言語を選択します。
- クリックを繰り返し、EULA を承認します。
- 「**1- Novell iManager 2.6, Tomcat, JVM**」を選択して iManager をインストールします。
- 「**1- Yes**」を選択してプラグインをダウンロードします。
- ダウンロードにデフォルトのパスを使う場合は [Enter] キーを押します。

インストールプログラムがインターネット上でダウンロードするサイトを検索します。この処理には数分かかることがあります。次に、どのプラグインをインストールしたいかを尋ねられます。

  - すべてのプラグインをダウンロードするには「**All**」を選択します。
  - 「**1- Yes**」を選択して自環境で使用可能なプラグインをインストールします。

- ダウンロードにデフォルトのパスを使う場合は [Enter] キーを押します。
- Apache を自動設定（オプション）させるには「**2- No**」を選択します。
- Tomcat にデフォルトポート（8080）を承認します。

- Tomcat にデフォルト SSL ポート（8443）を承認します。
- Tomcat にデフォルト JK コネクタポート（9009）を承認します。
- 適切な管理権限を持つ管理ユーザの ID（たとえば「root.fts」）を入力してください。
- 適切な管理権限を持つ管理ユーザの ツリー名（たとえば「fwlab」）を入力してください。
- 「**1-OK...**」と一緒に表示されたエントリの要約を承認してインストールを終了させます。

Novell iManager へのログイン

インストールが終わると、以下の URL からウェブブラウザ経由で iManager にログインできます。

https://<IP address of the eDirectory server>:8443/nps

i Novell のブラウザには Microsoft Internet Explorer または Mozilla Firefox を推奨します。Mozilla Firefox の場合、一度にすべてのコンテキストメニューのポップアップウィンドウを表示させないようにすることもできます。

ConsoleOne のインストールと起動

ConsoleOne は Novell _eDirectory のもう 1 つの管理ツールです。

ConsoleOne を以下のようにインストールしてください。

- ルート権限（スーパーユーザ）で eDirectory Server にログインします。
- ディレクトリ **/home/eDirectory** に移動します。

```
cd /home/eDirectory
```

- ConsoleOne のアーカイブ **c1_136f-linux.tar.gz** を解凍します。

```
tar -xzvf c1_136f-linux.tar.gz
```

  解凍すると、**/home/eDirectory** に **Linux** という新しいサブディレクトリが作られます。

- ディレクトリ **Linux** に進みます。

```
cd Linux
```

- インストール用スクリプト **c1-install** を呼び出します。

```
./c1-install
```

- インストール時のメッセージを出力する言語を選択します。
- 「8」を入力してすべてのスナップインをインストールしてください。

ConsoleOne にはインストール済みの Java ランタイム環境へのパスが必要です。対応するパス名を環境変数 **C1_JRE_HOME** にエクスポートすることができます。ただし、パス名をシステム全体にエクスポートするためには、**bash** プロファイルの変更が必要です。

> **i** ConsoleOne を操作するためには、原則として ID「**superuser Root**」をエクスポートできるレベルのルート権限が要求されます。パス名をシステム全体にエクスポートする方法は以下に紹介する通りです。すなわち、通常のユーザでもルート権限があれば ConsoleOne を操作することができます。

次の手順に従います。

► 編集する設定ファイルを開きます（この例では「**/etc/bash.bashrc**」）。

► 設定ファイルの「# End of ...」の前に次の行を入力します。

```
export C1_JRE_HOME=/opt/novell/j2sdk1.4.2_05/jre
```

eDirectory と同時にインストールされた java ランタイム環境をここで使用します。一方、eDirectory Server 上にインストールされたいずれかの Java ランタイム環境のパス名を指定することもできます。

ConsoleOne はローカルの設定ファイル **hosts.nds** または SLP サービスとマルチキャストを経由して使用可能なツリー階層を取得します。

以下のように、ユーザのツリー階層を設定ファイルに挿入してください。

► 設定用ディレクトリに移動します。

```
cd /etc
```

► ファイル **hosts.nds** がまだ存在しない場合には作成してください。

► ファイル **hosts.nds** を開いて以下の行を挿入します。

```
#Syntax: TREENAME.FQDN:PORT
MY_Tree.mycomputer.mydomain:81
```

ConsoleOne の起動

ConsoleOne はシステムプロンプトから以下のコマンドを使用して起動できます。

```
/usr/ConsoleOne/bin/ConsoleOne
```

7.2.6.3 Novell eDirectory の設定

以下の手順を実行して Novell eDirectory を設定してください。

1. NDS ツリーを作成します。
2. eDirectory の LDAP 用設定
3. LDAP Browser を経由した eDirectory への試験アクセス

NDS ツリーの作成

ユーティリティ ndsmanage を使用して **NDS**（**N**etwork **D**irectory **S**ervice : ネットワークディレクトリサービス）ツリーを作成します。このためには、ndsmanage で以下の情報が必要になります。

ツリー名
新しい NDS ツリーのネットワーク用の一意の名前、たとえば「**MY_TREE**」。

サーバ名
eDirectory 内の「**server**」クラスのインスタンス名。「**Server Name**」には、LDAP サーバが稼働している PRIMERGY サーバの名前を指定してください。たとえば、**lin36-root-0** と指定します。

サーバコンテキスト
server オブジェクトを格納するコンテナの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、**dc=organization.dc=mycompany**。

Admin ユーザ
管理を実行する許可を持つユーザの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、**cn=admin.dc=organization.dc=mycompany**。

NCP ポート
ポート 81 を指定してください。

インスタンスのロケーション
次のパスを指定します : **/home/root/instance0**

設定ファイル
次のファイルを指定します : **/home/root /instance0/ndsconf**

Admin ユーザのパスワード
管理者のパスワードをここに入力します。

次の手順で NDS ツリーを設定します。

▶ コマンドボックスを開きます。

▶ ディレクトリ **/home/eDirectory** に移動します。

▶ コマンド ndsmanage を入力してユーティリティ **ndsmanage** を起動します。

```
ndsmanage
```

▶ 「c」を入力して、クラス **server** の新しいインスタンスを生成します。

▶ 「y」を入力して設定作業を続けます。

▶ 「y」を入力して新しいツリーを作成します。

次に ndsmanage は、**TREE NAME**、**Server Name**、**Server Context** などの値を順に問い合わせます（180 ページを参照）。

入力が完了すると、NDS ツリーが ndsmanage によって設定されます。

▶ NDS ツリーの設定が終わったら、PRIMERGY サーバを再起動させて、設定の実効化、すなわち、NDS ツリーの再作成を行います。

LDAP 用の eDirectory の設定

eDirectory を LDAP 用に設定する手順は次の通りです。

– Role Based Services（RBS）をインストールします。

– プラグインモジュールの設定

– Role Based Services（RBS）の設定

– eDirectory の設定（SSL/TLS を使用する、もしくは使用しない）

以下の手順で個々の作業を完了させます。

▶ Web ブラウザを使用して、管理者 ID（**Admin**）で iManager にログインします。

Role Based Services（RBS）のインストール

iManager Configuration ウィザードを使用して RBS をインストールします。

次の手順に従います。

- ▶ iManager で、「**Configure**」タブを選択します（机のアイコンをクリックしてください）。
- ▶ 「**Configure**」タブで、次の順に選択します。
  「**Role Based Services**」-「**RBS Configuration**」
- ▶ RBS Configuration ウィザードを起動します。
- ▶ 管理を行うコンテナに **RBS2** を割り当てます。（上の例では「mycompany"」となっています。）

プラグインモジュールのインストール

次の手順に従います。

- ▶ iManager で、「**Configure**」タブを選択します（机のアイコンをクリックしてください）。
- ▶ 「**Configure**」タブで、次の順に選択します。
  「**Plug-in installation**」-「**Available Novell Plug-in Modules**」
- ▶ 「**Available Novell Plug-in Modules**」ページにリストされたモジュールから、eDirectory 専用のパッケージ **eDir_88_iMan26_Plugins.npm** を選択します。
- ▶ 「**インストール**」をクリックします。

Role Based Services（RBS）を設定します。

- ▶ 「**Available Novell Plug-in Modules**」ページで、LDAP 統合に必要なすべてのモジュールを選択してください。よくわからない場合は、すべてのモジュールを選択します。
- ▶ 「**インストール**」をクリックします。

eDirectory の SSL/TLS- セキュリティ保護されたアクセスの設定

i eDirectory のインストール中には、臨時の証明書が生成されますので、eDirectory へのアクセスは初期設定でも SSL/TLS によりセキュリティ保護されます。ただし、iRMC S2/S3 のファームウェアは RSA/MD5 証明書を使用するように設定されているので、SSL/TLS セキュリティ保護された eDirectory 経由のグローバル iRMC S2/S3 ユーザ管理には 1024 バイト長の RSA/MD5 証明書が必要です。

1024 バイト長の RSA/MD5 証明書は ConsoleOne を使用して以下のように作成します。

► 管理者 ID（**Admin**）を使用して LDAP サーバにログインし、ConsoleOne を起動してください。

► 社内ストラクチャのルートディレクトリに移動します（たとえば、**treename/mycompany/myorganisation**）。

► 「**New Object - NDSPKI key material - custom**」を選択して、クラス **NDSPKI:Key Material** の新しいオブジェクトを作成します。

► その後に表示されるダイアログで、以下の値を指定してください。

1. 1024 ビット
2. SSL または TLS
3. 署名 RSA/MD5

要求したタイプの署名が新しく作成されます。

新たに作成した証明書を SSL セキュリティ保護された LDAP 接続のために有効化するには、iManager で以下の作業を行います。

► ウェブブラウザから iManager を起動します。

► 有効な認証データを使用して iManager にログインします。

► **「LDAP」-「LDAP Options」-「LDAP Server」-「Connection」**の順に選択します。

「**Connection**」タブには、システム上でインストールされたすべての証明書を表示するドロップダウンリストがあります。

► ドロップダウンリストから必要な証明書を選択します。

eDirectory の SSL- セキュリティ保護されないアクセスの設定

eDirectory のデフォルト設定では匿名ログインやセキュリティ保護されないチャンネルを経由する平文表示のパスワードは無効となります。このため、eDirectory サーバにウェブブラウザでログインするには SSL 接続経由とするほかには方法がありません。

LDAP を SSL なしで使用したい場合は、以下の手順を実行しなければなりません。

1. SSL セキュリティ保護されない LDAP 接続の確立

2. バインド制限の緩和

3. LDAP 設定の再ロード

次の手順に従います。

1. SSL セキュリティ保護されない LDAP 接続の確立

    - ► ウェブブラウザから iManager を起動します。
    - ► 有効な認証データを使用して iManager にログインします。
    - ► 「**Roles and Tasks**」ビューを選択します。
    - ► **「LDAP」-「LDAP Options」-「LDAP Server」-「Connection」**の順に選択します。
    - ► 「**Connection**」タブで、以下のオプションを無効にします。
      Require TLS for all Operations
    - ► **「LDAP」-「LDAP Options」-「LDAP Group」-「General」**の順に選択します。
    - ► 「**General**」タブで、「**Require TLS for Simple Binds with password**」オプションを無効にします。

2. バインド制限の緩和

    - ► 有効な認証データを使用して iManager にログインします。
    - ► オブジェクトツリーで、**LDAP Server** オブジェクトに移動します。
    - ► マウスで **LDAP Server** オブジェクトをクリックしてハイライトさせ、関連するコンテキストメニューから「**Modify Object**」を選択します。
    - ► 右側のコンテントフレームで、「**Other**」シートを開きます。
    - ► 「**Valued Attributes**」で **ldapBindRestrictions** を選択します。
    - ► 「**編集**」ボタンをクリックします。
    - ► 値を「0」に設定します。
    - ► 「**OK**」をクリックします。
    - ► 「**Other**」シートで、「**適用**」ボタンをクリックします。

3. LDAP 設定の再ロード

    - ► ConsoleOne を起動して eDirectory にログインします。
    - ► ウィンドウの左側にある **Base DN** オブジェクト（たとえば **Mycompany**）をクリックします。すると、**LDAP server** オブジェクトがウィンドウの右側に表示されます。

- 右クリックして **LDAP Server** オブジェクトをハイライトさせ、関連するコンテキストメニューから「**Properties**」を選択します。
- 「**General**」タブで、「**Refresh NLDAP Server Now**」をクリックします。

LDAP ブラウザでの eDirectory アクセス試験

以上 1 から 3 までの手順に成功したら、LDAP ブラウザユーティリティを使用して eDirectory への接続が確立しなければなりません。Jarek Gavor 氏 の LDAP ブラウザ（202 ページを参照）を使用して、以下のようにこの接続の試験をします。

- 管理者 ID

  （たとえば **admin**）を使用して SSL 接続で eDirectory にログインできるか試してみます。

この接続に失敗した場合は、以下のようにしてください。

- SSL が有効であることを確認します（183 ページを参照）。

図 54: eDirectory への LDAP 接続の試験：SSL 有効時

- 管理者 ID

  （たとえば **admin**）を使用して非 SSL セキュア接続で eDirectory にログインできるか試してみます。

図 55: eDirectory への LDAP 接続の試験 : SSL 無効時

► ログインが再度失敗する場合は、
バインド制限の緩和（183 ページを参照）。

7.2.6.4 iRMC S2/S3 ユーザ管理の Novell eDirectory への統合

前提条件 :

LDAP v2 ストラクチャが eDirectory ディレクトリサービスですでに生成されていること（152 ページ の「SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除」の項を参照）。

以下の手順を実行して、iRMC S2/S3 ユーザ管理を Novell eDirectory に統合します。

– iRMC プリンシパルユーザの作成

– eDirectory の iRMC グループとユーザ権限の宣言

– ユーザの許可グループへの割り当て

eDirectory の iRMC S2/S3 LDAP ユーザ LDAP 認証プロセス

グローバル iRMC S2/S3 ユーザが iRMC S2/S3 にログインする際の認証は、定義済みのプロセスに従って処理されます（140 ページを参照）。187 ページ の図 56 では、この認証プロセスを、Novell eDirectory のグローバル iRMC S2/S3 ユーザ管理に関して図解します。

対応するログイン情報による接続とログインの確立を、BIND 操作と呼びます。

1) iRMC S2/S3 は、「Principal User」という定義済みで既知のアクセス許可データ（iRMC S2/S3 設定）を使用して eDirectory サーバにログインし、正しくバインドされるのを待ちます。

2) iRMC S2/S3 は eDirectory サーバに「cn=User1」でユーザの完全修飾識別された識別名（DN）を提供するようにリクエストします。eDirectory は定義済みのサブツリー（iRMC S2/S3 設定）から DN を決定します。

3) iRMC S2/S3 はユーザ User1 の完全修飾 DN を使用して eDirectory サーバにログインし、正常にバインドされるのを待ちます。

4) iRMC S2/S3 は eDirectory サーバにユーザ User1 のユーザ権限を付与するようにリクエストします。

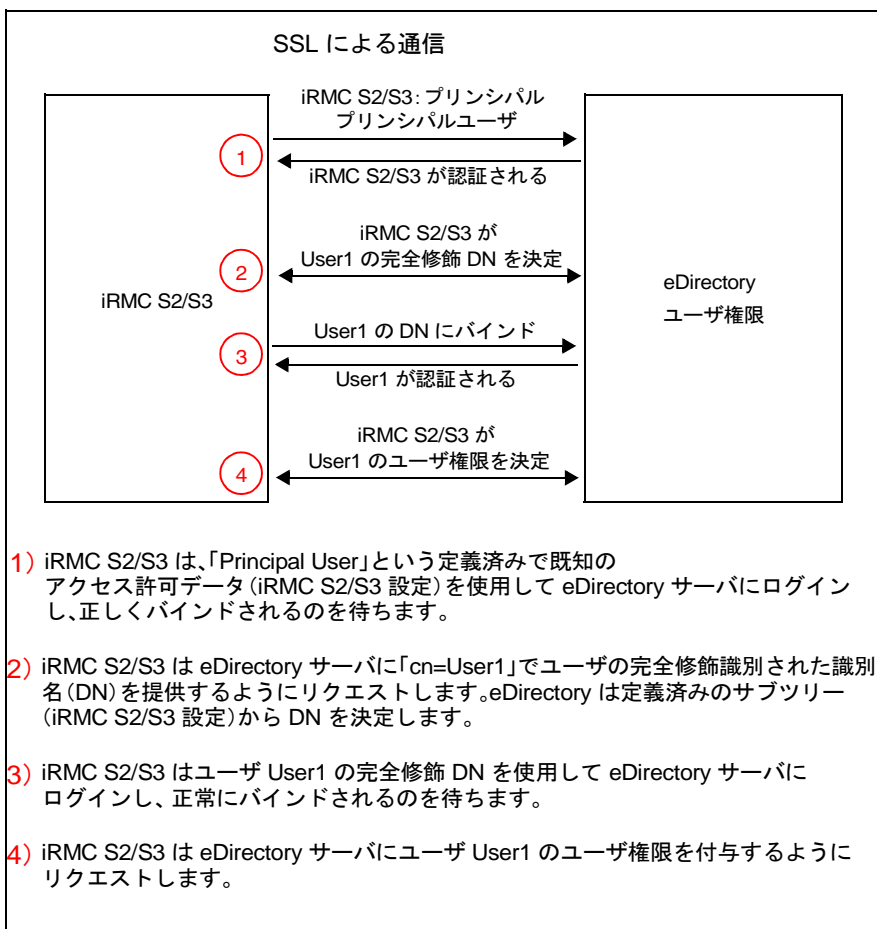



図 56: グローバル iRMC S2/S3 権限の認証ダイアグラム

> **i** 「プリンシパルユーザ」権限データと DN を含むサブツリーは、iRMC S2/S3 の Web インターフェースの「**Directory Service Configuration**」ページで設定します（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』を参照）。

> **i** ユーザの CN は、検索されるサブツリーの中で一意でなければなりません。

iRMC S2/S3 用のプリンシパルユーザの作成

iRMC S2/S3 用のプリンシパルユーザを以下の通り作成します。

- ▶ 有効な認証データを使用して iManager にログインします。
- ▶ 「**Roles and Tasks**」を選択します。
- ▶ 「**Users - Create User**」を選択します。
- ▶ 表示されるテンプレートに必要な項目を入力します。

  > **i** プリンシパルユーザの識別名（DN）とパスワードは対応する iRMC S2/S3 の設定の項目に一致する必要があります（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』を参照）。
  >
  > ユーザの「**Context:**」はツリーのどの位置にあっても構いません。

- ▶ 以下のサブツリーにプリンシパルユーザの検索許可を割り当てます。
  - サブツリー（OU）**SVS**
  - ユーザを含むサブツリー（OU）（たとえば「**people**」）

iRMC グループとユーザへのユーザ権限の割り当て

デフォルト設定では、eDirectory のオブジェクトには、LDAP ツリー内の非常に限定されたクエリと検索の許可しかありません。ひとつまたは複数のサブツリーのすべての属性をオブジェクトがクエリできるようにするには、このオブジェクトに対応する許可を割り当てる必要があります。

許可は個々のオブジェクト（すなわち個々のユーザ）に割り当てることもできますし、同じ組織単位（OU）の中で照合されるオブジェクトのグループ（「**SVS**」または **people**。この場合、OU に割り当てられ、「引き継がれた」と識別された許可は、このグループのオブジェクトに自動的に認定されます。

> **i** iRMC S2/S3 ユーザ管理と Novell eDirectory を統合するには、次のオブジェクト（トラスティ）に検索の許可を割り当てる必要があります。
>
> – **プリンシパルユーザ**
> – iRMC S2/S3 ユーザが含まれるサブツリー
>
> 以下にこの操作を詳しく説明します。

すべての属性に関するオブジェクト検索許可を割り当てるプロセスは以下の通りです。

► ウェブブラウザから iManager を起動します。

► 有効な認証データを使用して iManager にログインします。

► iManager で、「**Roles and Tasks**」ボタンをクリックします。

► メニューツリーストラクチャで、「**Rights**」**-**「**Rights to Other Objects**」の順に選択します。

「**Rights to Other Objects**」ページが表示されます。

► 「**Trustee Name**」の下に、アクセス許可を許可するオブジェクトの名前を指定します（190 ページ の図 57 の「**SVS.sbdr4**」）。

► 「**Context to Search From**」で、eDirectory のサブツリー（**SVS**）を指定します。iManager ははこのサブツリーから、トラスティ「**Users**」が現在読み取りの許可を持っているオブジェクトを検索します。

► 「**OK**」をクリックします。

進捗ディスプレイに検索の状況が表示されます。検索作業か終了すると、「**Rights to Other Objects**」ページに検索結果が表示されます（190 ページ の図 57 を参照）。

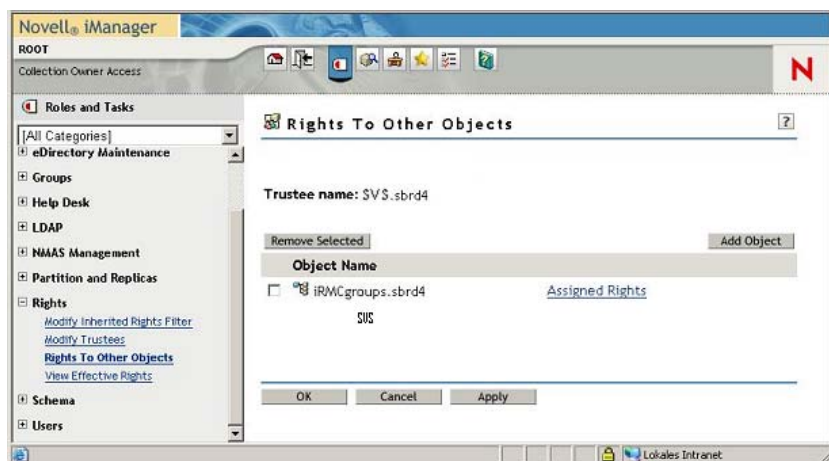



図 57: iManager - ロールとタスク - 他のオブジェクトに対する権限

i 「**Object Name**」の下に何もオブジェクトが表示されない場合、トラスティには指定されたコンテキストの範囲内に許可はありません。

► 必要に応じてトラスティに追加の許可を割り当ててください。

► 「**Add Object**」をクリックします。

► オブジェクトセレクタボタンを使用して、トラスティに許可を割り当てたいオブジェクトを選択します。

► 「**Assigned Rights**」をクリックします。

プロパティ「**All Attributes Rights**」が表示されない場合 :

► 「**Add Property**」をクリックします。

「**Add Property**」ウィンドウが表示されます（191 ページ の図 58 を参照）。

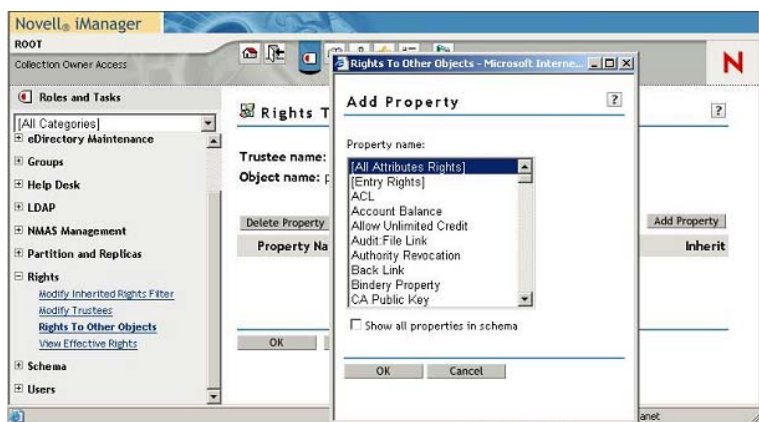



図 58: iManager - ロールとタスク - 他のオブジェクトに対する権限？プロパティの追加

- ► プロパティ「**All Attributes Rights**」をハイライトさせ、「**OK**」をクリックして追加します。

► プロパティ「**All Attributes Rights**」に対し、オプション「**Compare**」、「**Read**」、「**Inherit**」を有効にし、「**OK**」をクリックして確定します。

この操作によって、ユーザまたはユーザグループに、選択されたオブジェクトのサブツリーの属性をすべてクエリする権限が与えられます。

► 「**適用**」をクリックして、設定を有効にします。

7.2.6.5 iRMC S2/S3 ユーザの許可グループへの割り当て

iRMC S2/S3 ユーザを（たとえば OU「**people**」から）次のいずれの方法でも iRMC 許可グループに割り当てる事ができます。

– ユーザエントリから開始（ユーザエントリの数がごく少ない場合はこの方が適当）
– または、ロールエントリ／グループエントリから開始（ユーザエントリの数が多い場合はこの方が適当）

i 次の例は iRMC S2/S3 ユーザを OU「**people**」から許可グループに割り当てる方法を示します。割り当てをロールエントリ／グループエントリから開始する方法を説明しています。

ユーザエントリに基づく割り当て方法もほぼ同じです。

i eDirectory 内のグループにユーザを「手作業」で入力する必要があります。

次の手順に従います。

▶ ウェブブラウザから iManager を起動します。

▶ 有効な認証データを使用して iManager にログインします。

▶ 「**Roles and Tasks**」を選択します。

▶ 「**Groups - Modify Group**」を選択します。

「**Modify Group**」ページが表示されます。

▶ iRMC S2/S3 ユーザを割り当てたいすべての許可グループについて次の作業を実行します。

▶ オブジェクトセレクタボタンを使用して、 iRMC S2/S3 ユーザを追加したい許可グループを選択します。LDAP v2 ストラクチャの例（193 ページ の図 59 を参照）ではこの操作は、**Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4**。

► 「メンバ」タブを選択します。

「**Modify Group**」ページの「**Members**」タブが表示されます。

図 59: 「iManager」-「Roles and Tasks」-「Modify Group」-「Members」タブ（LDAP v2）

► iRMC グループに割り当てたい OU「**people**」のすべてのユーザについて、次の作業を実行します。

► オブジェクトセレクタボタンをクリックします。 と共に提供されます。

「**Object Selector**（**Browser**）」ウィンドウが開きます（194 ページ の図 60 を参照）。

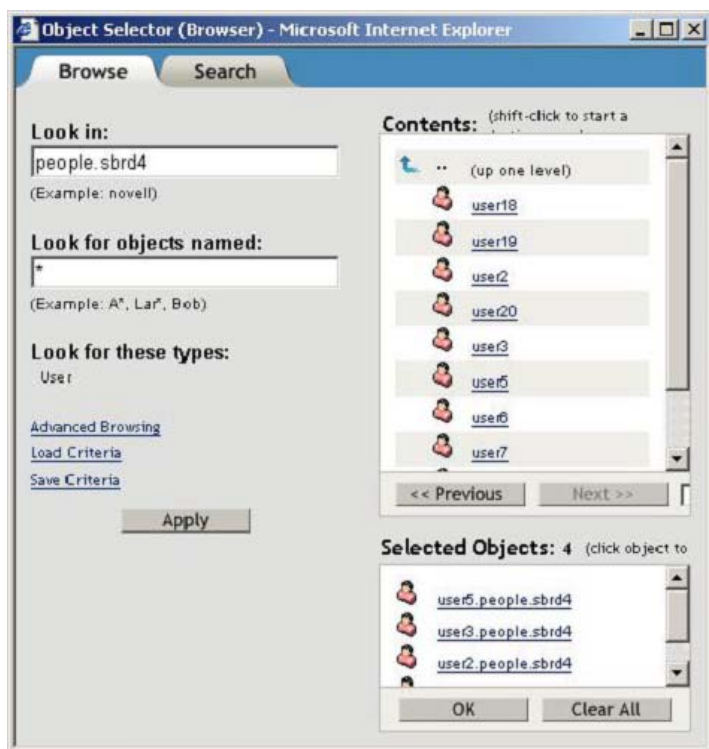



図 60: iRMC グループへのユーザの割り当て - ユーザの選択

► 「**Object Selector**（**Browser**）」ウィンドウで、OU「**people**」の中の必要なユーザを選択し、「**OK**」をクリックして確定します。

選択されたユーザは「**Modify Group**」ページの「**Members**」タブの表示領域にリストされています（193 ページ の図 59 を参照）。

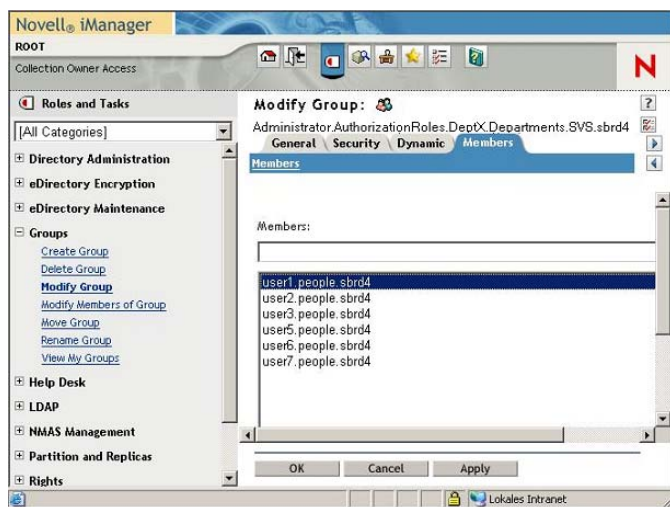



図 61: 「Members LDAP v2」タブが選択された iRMC S2/S3 ユーザ表示

► 選択されたユーザが iRMC グループに追加されるように、「**Apply**」または「**OK**」で確定します（この例では **....SVS.sbdr4**）。

7.2.6.6 Novell eDirectory 管理のためのヒント

NDS デーモンの再起動

次の手順で NDS デーモンを再起動します。

- ► コマンドボックスを開きます。
- ► ルート許可でログインします。
- ► 次のコマンドを実行します。

```
rcndsd restart
```

nldap デーモンの再起動に失敗し、理由が分からない場合

- ► **nldap** デーモンを「手作業」で起動します。

```
/etc/init.d/nldap restart
```

iManager から応答がない場合

- ► iManager を再起動してください。

```
/etc/init.d/novell-tomcat4 restart
```

NLDAP サーバ設定の再ロード

次の手順に従います。

- ► ConsoleOne を起動して eDirectory にログインします。

ConsoleOne を初めて立ち上げる場合は、ツリーが設定されていません。

以下の手順でツリーを設定してください。

- ► 「**My World**」の下のノード「**NDS**」を選択します。
- ► メニューバーから「**File**」**-**「**Authenticate**」の順に選択します。
- ► 次のログイン用認証データを入力します。

1. ログイン名：root
2. パスワード： <password>
3. ツリー : MY_TREE
4. コンテキスト：mycompany

► ウィンドウの左側部分で、「**Base DN**」オブジェクト（**Mycompany**）をクリックします。

すると、「**LDAP Server**」オブジェクトがウィンドウの右側に表示されます。

► 「**LDAP Server**」オブジェクトを右クリックし、コンテキストメニューで「**Properties**」を選択します。

► 「**General**」タブで、「**Refresh NLDAP Server Now**」ボタンをクリックします。

NDS メッセージトレースの設定

nds デーモンは、デバッグメッセージとログメッセージを生成します。このメッセージは **ndstrace** ツールを使用してトレースすることができます。以下に説明する設定の目的は、**ndstrace** からの出力をファイルにリダイレクトし、他のターミナルでこのファイルの内容を表示させることです。後者の作業には **screen** ツールを使用します。

以下の手順を推奨します。

► コマンドボックス（たとえば **bash**）を開きます。

ndstrace を設定します。

► eDirectory のディレクトリ **/home/eDirectory** に移動します。

```
cd /home/eDirectory
```

► `screen` コマンドを使用して **screen** を起動します。

► `ndstrace` コマンドを使用して **ndstrace** を起動します。

► 有効化したいモジュールを選択します。

たとえば、イベントが発生した時間を表示したい場合は、「`dstrace TIME`」と入力します。

LDAP および **TIME** モジュールを有効化するには、以下を入力することを強く推奨します。

```
dstrace LDAP TIME
```

► **quit** と入力して **ndstrace** を終了します。

これで **ndstrace** の設定は終了しました。

別のターミナルでのメッセージの出力

- **ndstrace** を起動して、メッセージ出力をリダイレクトします。

```
ndstrace -l >ndstrace.log
```

- 以下のキーの組み合わせを使用して別のターミナルを開きます。
  [Ctrl] + [[a]]、Ctrl + [c]

- ログの記録を開始します。

```
tail -f ./ndstrace.log
```

- 仮想端末を切り替えるには、キーの組み合わせ [Ctrl] + [a]、[Ctrl] + [0] を使用します。
  （ターミナルには 0 から 9 までの番号が付きます。）

7.2.7 OpenLDAP によるグローバル iRMC S2/S3 ユーザの管理

この節では次の点について説明します。

- OpenLDAP（Linux）のインストール
- SSL 証明書の作成
- OpenLDAP の設定。
- iRMC S2/S3 ユーザの管理の OpenLDAP への統合
- OpenLDAP 管理のヒント

7.2.7.1 OpenLDAP のインストール

i OpenLDAP をインストールする前に、ファイヤーウォールをポート 389 と 636 に接続できるように設定する必要があります。

OpenSuSE の場合は以下の手順に従います。

► ファイル **/etc/sysconfig/SuSEfirewall2** で、オプション **FW_SERVICES_EXT_TCP** を次のように拡張します。

```
FW_SERVICES_EXT_TCP=“389 636”
```

配布媒体から取得したパッケージ **OpenSSL** および **OpenLDAP2** をインストールするときは、セットアップツール YaST を使用してください。

7.2.7.2 SSL 証明書の作成

次のプロパティを持つ証明書を作成する必要があります。

- 鍵の長さ : 1024 ビット
- md5RSAEnc

鍵ペアと署名入り証明書（自己署名または外部 CA の署名）の作成には OpenSSL を使用します。より詳しい情報は OpenSSL のホームページ、*http://www.openssl.org* を参照してください。

CA の設定とテスト証明書の作成の説明書は以下のリンクから入手してください。

- *http://www.akadia.com/services/ssh_test_certificate.html*
- *http://www.freebsdmadeeasy.com/tutorials/web-server/apache-ssl-certs.php*
- *http://www.flatmtn.com/computer/Linux-SSLCertificates.html*
- *http://www.tc.umn.edu/~brams006/selfsign.html*

証明書の作成に続いて、以下の 3 個の PEM ファイルを入手してください。

– ルート証明書 : **root.cer.pem**

– サーバ証明書 : **server.cer.pem**

– 秘密鍵 : **server.key.pem**

> i 秘密鍵は決してパスフレーズで暗号化**しないでください。**
> **server.key.pem** ファイルには、LDAP デーモン（**ldap**）読み取り許可**のみが割り当てられる**ためです。
>
> 次のコマンドを使用してパスフレーズを削除してください。
>
> ```
> openssl rsa -in server.enc.key.pem -out server.key.pem
> ```

7.2.7.3 OpenLDAP の設定

次の手順で OpenLDAP を設定します。

► Yast セットアップツールを起動させ、「**LDAP-Server-Configuration**」を選択します。

► 「**Global Settings/Allow Settings**」で **LDAPv2-Bind** の設定を有効にします。

► 「**Global Settings/TLS Settings**」を選択します。

  ► **TLS** 設定を有効にします。

  ► インストール時に作成されたファイルのパスを宣言してください（199 ページ の「OpenLDAP のインストール」の項 を参照）。

  ► ファイルシステムの証明書と秘密鍵を読み取ることができるのは LDAP サービスのみであることを確認してください。

  openldap は **uid/guid=ldap** の下で実行されるので、確認は以下の方法で行うことができます。

  – ファイルのオーナーの証明書と秘密鍵を「ldap」に設定する

  – または、LDAP デーモン **ldap** の読み取り許可を証明書と秘密鍵が入ったファイルに割り当てる

► 「**Databases**」を選択して新しいデータベースを作成します。

i YaST で作成した設定が全体的に機能しない場合には、以下の必須エントリがファイル **/etc/openldap/slapd.conf** にあるかを確認してください。

```
allow bind_v2
TLSCACertificateFile /path/to/ca-certificate.pem
TLSCertificateFile /path/to/certificate.pem
TLSCertificateKeyFile /path/to/privat.key.pem
```

i YaST で作成した SSL の設定が機能しない場合は、以下のエントリが設定ファイル **/etc/sysconfig/openldap** にあるかを確認してください。

```
OPENLDAP_START_LDAPS=“yes”
```

7.2.7.4 iRMC S2/S3 ユーザの管理の OpenLDAP への統合

前提条件：

LDAP v2 ストラクチャが OpenLDAP ディレクトリサービスのなかに生成済みであること（152 ページ の「SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除」の項を参照）。

iRMC S2/S3 ユーザ管理の OpenLDAP への統合は以下の手順で行います。

– iRMC プリンシパルユーザの作成

– 新規 iRMC S2/S3 ユーザの作成とそのユーザに対する許可グループの割り当て

プリンシパルユーザ（ObjectClass : **Person**）を作成するには、Jarek Gawor 氏作の LDAP Browser\Editor などの LDAP ブラウザ（202 ページ を参照）を使用します。

Jarek Gawor 氏の著作による LDAP Browser\Editor

Jarek Gawor 氏の著作による LDAP Browser\Editor はグラフィカルユーザインターフェースによる使いやすいものです。

このツールはインターネットでダウンロードできます。

以下の手順で **LDAP Browser\Editor をインストール**してください。

► 圧縮アーカイブ **Browser281.zip** を任意のインストール用ディレクトリで解凍します。

► JAVA ランタイム環境用の環境変数 **JAVA_HOME** をインストール用ディレクトリに設定します。たとえば、以下のようにします。

```
JAVA_HOME=C:\Program Files\Java\jre7
```

プリンシパルユーザの作成

プリンシパルユーザ（ObjectClass : **Person**）を作成するには、Jarek Gawor 氏作の LDAP Browser\Editor などの LDAP ブラウザ（202 ページ を参照）を使用します。

以下に、Jarek Gawor 氏の LDAP Browser\Editor を用いてプリンシパルユーザを作成する方法を説明します。

次の手順に従います。

- ► LDAP ブラウザを起動します。
- ► 有効な認証データを使用して OpenLDAP ディレクトリサービスにログインします。
- ► プリンシパルユーザを作成するサブツリー（サブグループ）を選択します。プリンシパルユーザはサブツリー内のどこにでも作成できます。
- ► 「**編集**」メニューを開きます。
- ► 「**Add Entry**」を選択します。
- ► 「**Person**」を選択します。
- ► 識別名 **DN** を編集します。

  プリンシパルユーザの識別名（DN）とパスワードは対応する iRMC S2/S3 の設定の項目に一致する必要があります（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』を参照）。

- ► 「**Set**」をクリックしてパスワードを入力します。
- ► 苗字 **SN** を入力します。
- ► 「**Apply**」をクリックします。

新規 iRMC S2/S3 ユーザの作成とそのユーザに対する許可グループの割り当て

i 新規ユーザ（ObjectClass **Person**）の作成とユーザの許可グループへの割り当てには、LDAP ブラウザ、たとえば Jarek Gawor 氏が作成した LDAP Browser\Editor などを使用します（202 ページを参照）。

以下に、Jarek Gawor 氏の LDAP Browser\Editor を用いて新規の iRMC S2/S3 ユーザを作成し、そのユーザを許可グループに割り当てる方法を説明します。

次の手順に従います。

- LDAP ブラウザを起動します。
- 有効な認証データを使用して OpenLDAP ディレクトリサービスにログインします。
- 新規ユーザを作成します。

  これは次の手順で行います。

  - 新規ユーザを作成するサブツリー（サブグループ）を選択してください。新規ユーザはサブツリー内のどこにでも作成できます
  - 「**編集**」メニューを開きます。
  - 「**Add Entry**」を選択します。
  - 「**Person**」を選択します。
  - 識別名 **DN** を編集します。
  - 「**Set**」をクリックしてパスワードを入力します。
  - 苗字 **SN** を入力します。
  - 「**Apply**」をクリックします。

► 今作成したユーザを許可グループに割り当てます。

これは次の手順で行います。

- ► ユーザを所属させる **SVS** サブツリー（サブグループ）を次のように選択します。

  cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

- ► 「**編集**」メニューを開きます。
- ► 「**Add Attribute**」を選択します。
- ► 属性名として「Member」を指定します。値にはここで作成したユーザの完全修飾 DN を次のように指定してください。

  cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

7.2.7.5 OpenLDAP 管理のヒント

LDAP サービスの再起動

次の手順で LDAP サービスを再起動します。

▶ コマンドボックスを開きます。

▶ ルート許可でログインします。

▶ 次のコマンドを入力します。

```
rcldap restart
```

メッセージログの記録

LDAP デーモンは Syslog プロトコルを使用してメッセージログを記録します。

> i 記録されたメッセージは、ファイル **/etc/openldap/slapd.conf** でログレベルが 0 以外に設定されている場合にのみ表示されます。
>
> 各レベルの説明は下記を参照してください。
>
> *http://www.zytrax.com/books/ldap/ch6/#loglevel*

207 ページ の表 35 に、ログレベルとその意味の概要を記載しています。

ログレベル	意味
-1	全面的なデバッグ実行
0	デバッグ実行なし
1	ログファンクションコール
2	試験パケットの取扱い
4	ヘビートレースデバッグ実行
8	接続管理
16	送信 / 受信パケット表示
32	フィルタ処理の検索
64	設定ファイル処理
128	アクセス制御リスト処理
256	接続／操作／イベントのステータスログの記録
512	送信済みエントリのステータスログの記録
1024	シェルバックエンドによる出力通信
2048	エントリパースの出力結果

表 35: OpenLDAP - ログレベル

7.2.8 グローバル iRMC S2/S3 ユーザ宛ての Email 警告の設定

グローバル iRMC S2/S3 ユーザ宛の Email 警告が、グローバル iRMC S2/S3 ユーザ管理システムに組み込まれています。すなわち、1 台のディレクトリサーバを使用して、Email 警告をすべてのプラットフォーム向けに集中的に設定し操作することができます。適切に設定されたグローバルユーザ ID は、ネットワーク上でディレクトリサーバに接続されたすべての iRMC S2/S3 から Email 警告を受け取ることができます。

前提条件

Email 警告には、以下の要件を満たす必要があります。

– グローバル Email 警告には、LDAP v2 のストラクチャとしてバージョン 3.77A 以降の iRMC S2/S3 ファームウェアが必要です。

– プリンシパルユーザが iRMC S2/S3 Web インターフェースで設定され、LDAP ツリー内で検索する権限が付与されているる必要があります（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』を参照）。

– LDAP 設定を「**ディレクトリサービス構成**」ページで設定する際（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』を参照）、E-mail 設定を「**ディレクトリサービス E-mail 警告構成**」で有効にしておく必要があります。

7.2.8.1 グローバル Email 警告

ディレクトリサーバ経由のグローバル Email 警告には警告ロールが必要です。この警告ロールは管理ロールに加えて **SVS_LdapDeployer** の設定ファイル（152 ページを参照）で定義されます。

警告グループ（警告ロール）の表示

警告ロールは警告タイプ（たとえば、温度のしきい値を超えた、など）をまとめてグループ化しますが、それぞれに重要度（たとえば「致命的」）が割り当てられています。ユーザを特定の警告グループに割り当てると、ユーザが Email で受け取る警告のタイプと重大度が指定されます。

警告ロールの構文はサンプル設定ファイル **Generic_Settings.xml** と **Generic_InitialDeploy.xml** に具体的に解説されています。これらのファイルは、ServerView Suite DVD 1 に収録される **jar** アーカイブ **SVS_LdapDeployer.jar** に付属しています。

警告タイプの表示

以下の警告タイプがサポートされます。

警告タイプ	原因
FanSens	冷却ファンセンサ
Temperat	温度センサ
HWError	致命的なハードウェア故障
セキュリティの設定	セキュリティの設定
SysHang	システムのハング
POSTErr	POST エラー
SysStat	システムステータス
DDCtrl	ディスクドライブとコントローラ
NetInterf	ネットワークインターフェース
RemMgmt	リモートマネジメント
SysPwr	電源管理
メモリ	メモリ
その他	その他

表 36: 警告タイプ

各々の警告タイプには以下の重大度のいずれかが割り当てられます : **警告**、**致命的**、**すべて**、**(なし)**。

優先メールサーバ

グローバル Email 警告には、優先メールサーバの「**Automatic** 設定が適用されます。Email が即時に送ることができない場合、たとえば 1 番目のメールサーバが使用不可能な場合には、Email は 2 番目のメールサーバに送られます。

サポートされるメールフォーマット

以下の Email フォーマットがサポートされています。

– 標準
– 題名固定
– ITS フォーマット
– Fujitsu REMCS フォーマット

i **標準**以外のメールフォーマットを使用する場合は、対応するメールフォーマットグループにユーザを追加しなければなりません。

LDAP Email テーブル

Email 警告が設定され（212 ページを参照）、「**LDAP E-mail 通知を有効にする**」オプション（『iRMC S2/S3 - integrated Remote Management Controller』マニュアルを参照）が選択されている場合は、iRMC S2/S3 は警告が発行されると以下のユーザに Email を送信します。

– 適切に設定されたすべてのローカル iRMC S2/S3 ユーザ

– この警告のための LDAP Email テーブルに登録されているすべての iRMC S2/S3 ユーザ

LDAP Email テーブルは、iRMC S2/S3 が初回に起動されたときに、iRMC S2/S3 ファームウェアにより最初に作成され、定期的に更新されます。LDAP Email テーブルのサイズは、最大 64 の LDAP 警告ロールと、Email 警告の送信先に設定されている最大 64 のグローバル iRMC S2/S3 ユーザに限定されています。

i グローバル Email 警告には Email 配布リストの使用を推奨します。

LDAP ディレクトリサーバは、Email 警告の目的で、以下の情報を Email テーブルから取得します。

- Email 警告が設定されたグローバル iRMC S2/S3 ユーザのリスト
- 各グローバル iRMC S2/S3 ユーザに対して :
  - 警告タイプ毎に設定された警告のリスト（タイプと重大度）
  - 要求されたメールフォーマット

LDAP Email テーブルは以下の状況で更新されます。

– iRMC S2/S3 が初回に起動、または再起動されたとき

– LDAP の設定が変更されたとき

– 定期的（任意）更新の間隔は、iRMC S2/S3 Web インターフェースでの LDAP 設定の一部として「**LDAP 警告テーブルを更新する**」オプションで指定します（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』および「**LDAP 警告テーブルを更新する**」オプションを参照）。

ディレクトリサーバ上のグローバル Email 警告の設定

この節ではディレクトリサーバ上に LDAP Email 警告を設定する方法を説明します。

> 設定は、iRMC S2/S3 上にも行う必要があります。これは、iRMC S2/S3 Web インターフェースで設定します（マニュアル『iRMC S2/S3 - integrated Remote Management Controller』を参照）。

次の手順に従います。

- ディレクトリサービスに Email 警告を送信するユーザの Email アドレスを入力します。

  > Email アドレス設定に使用する方法は、運用するディレクトリサービス（Active Directory、eDirectory または OpenLDAP）によって異なります。

- 警告ロールを定義する設定ファイルを作成します。
- この設定ファイルを使用して **SVS_LdapDeployer** を起動し、対応する LDAP v2 ストラクチャ（**SVS**）をディレクトリサーバ上に生成させます（153 ページと 159 ページを参照）。

7.2.8.2 警告ロールの表示

LDAP v2 ストラクチャが生成されると、新たに作成された OU「**SVS**」が表示されます。たとえば、Active Directory では、**Declarations** の配下にコンポーネント **Alert Roles** および **Alert Types** と一緒に、また **DeptX** の配下にコンポーネント **Alert Roles** と一緒に表示されます（図 62 を参照）。

– **Declarations** の配下では、**Alert Roles** にすべての定義された警告ロールが表示され、**Alert Types** の下にすべての警告タイプが表示されます（1）。

– **DeptX** の配下では、**Alert Roles** の下に OU「**DeptX**」において有効なすべての警告ロールが表示されます（2）。

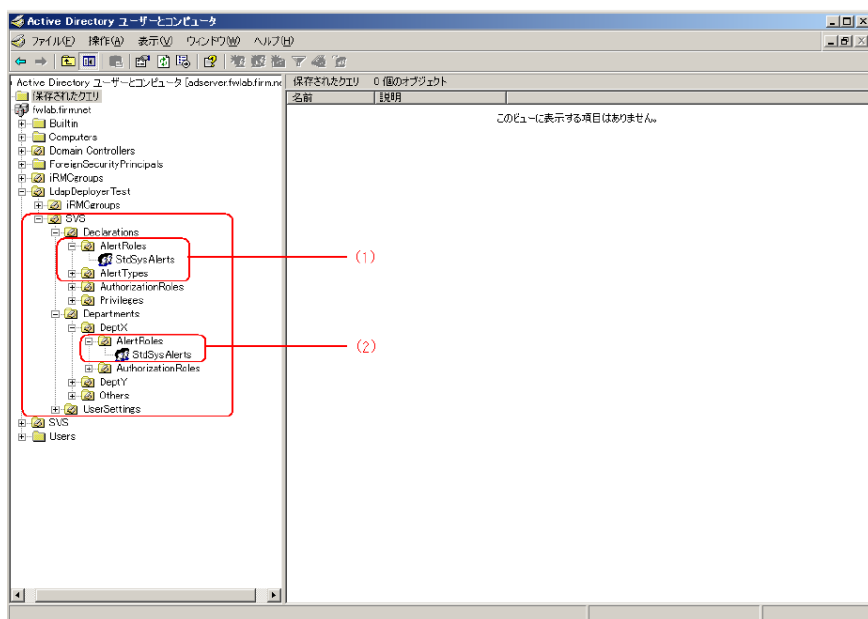



図 62: OU「SVS」と警告ロール

> **i** 個々の警告ロールのユーザに Email が確実に送信されるようにするため、関連部門を iRMC S2/S3 に設定する必要があります（図 62 の **DeptX**）（『iRMC S2/S3 - integrated Remote Management Controller』マニュアルを参照）。

「Active Directory ユーザとコンピュータ」のストラクチャツリーで**「SVS」–「Departments」–「DeptX」–「Alert Roles」**の下にある警告ロール（たとえば**「StdSysAlerts」**）を選択し（図 63 を参照）（1）、コンテキストメニューから**「プロパティ」–「メンバ」**を選択して**「プロパティ」**ダイアログボックスを開くと、その警告ロール（この例では**「StdSysAlerts」**）が**「メンバ」**タブの中に表示されます（2）。

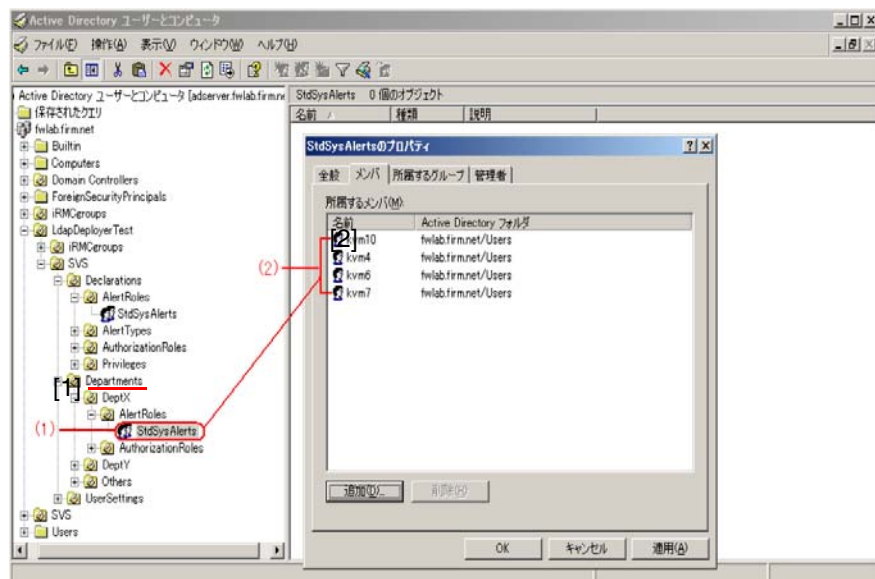



図 63: 警告ロール「StdSysAlert」に割り当てられたユーザ

7.2.8.3 iRMCS2/S3 ユーザへの警告ロール割り当て

iRMC S2/S3 ユーザに、以下のいずれかの方法で警告ロールを割り当てる事ができます。

– ユーザエントリに基づいて
– または、ロールエントリに基づいて

各種ディレクトリサービス（Microsoft Active Directory、Novell eDirectory および OpenLDAP）において、iRMC S2/S3 への 警告ロールの割り当ては、iRMC S2/S3 ユーザへ権限ロール（Authorization roles）を割り当てられるのと同じ方法で、同じツールを使用して行われます。

たとえば、Active Directory の場合は、「**Active Directory ユーザとコンピュータ**」スナップインの「**プロパティ**」ダイアログボックスの中の「**追加**」をクリックして割り当てを行います。（214 ページ の図 63 を参照）

7.2.9 SSL copyright

iRMC S2/S3-LDAP の統合には、OpenSSL プロジェクトに基づき Eric Young 氏が開発した SSL 実装を使用します。

```
/* ====================================================================
 * Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

8 付録 2 - LDAP ディレクトリサービスによるグローバル iRMC S4 ユーザ管理

iRMC S4 によるユーザ管理には 2 種類の異なるユーザ ID を使用します。

– **ローカルユーザー ID** は iRMC S4 内部の不揮発性記憶装置に保存され、iRMC S4 のユーザインターフェース経由で管理されます。

– **グローバルユーザ ID** はディレクトリサービスの集中データストアに保存され、ディレクトリサービスのインターフェース経由で管理されます。

  グローバル iRMC S4 ユーザ管理では、現在以下のディレクトリサービスがサポートされます。

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP[OpenLDAP]
  – OpenDS / OpenDJ / ApacheDS

本章では以下について説明します。

– iRMC S4 によるユーザ管理の概念
– ユーザ権限
– iRMC S4 上のグローバルユーザ管理

i iRMC S4 のローカルユーザ管理の詳細については、『iRMC S4 - integrated Remote Management Controller』マニュアルを参照してください。

i JBoss で実行される ServerView の内部ディレクトリサービス OpenDS では、iRMC S4 の**電子メール設定**機能はサポートされません。

8.1 iRMC S4 によるユーザ管理の概念

iRMC S4 によるユーザ管理は、ローカルとグローバルのユーザ ID を並列に管理することができます。

ユーザがいずれかの iRMC S4 のインターフェースにログインするために入力する認証データ（ユーザ名、パスワード）を検証する際には、iRMC S4 は以下のように処理します（合わせて 221 ページ の図 64 も参照してください）。

1. iRMC S4 はユーザ名とパスワードを内部に保存されたユーザ ID と照合します。
   - ユーザは、iRMC S4 認証に成功すれば（ユーザ名とパスワードが有効）ログインすることができます。
   - 認証に失敗した場合には、iRMC S4 はステップ 2 の検証手順を継続します。
2. iRMC S4 はユーザ名とパスワードを使用して、LDAP 経由でディレクトリサービスの認証を受け、LDAP クエリによってユーザの権限を判断してユーザに iRMC S4 を操作する権限があるかどうかを確認します。

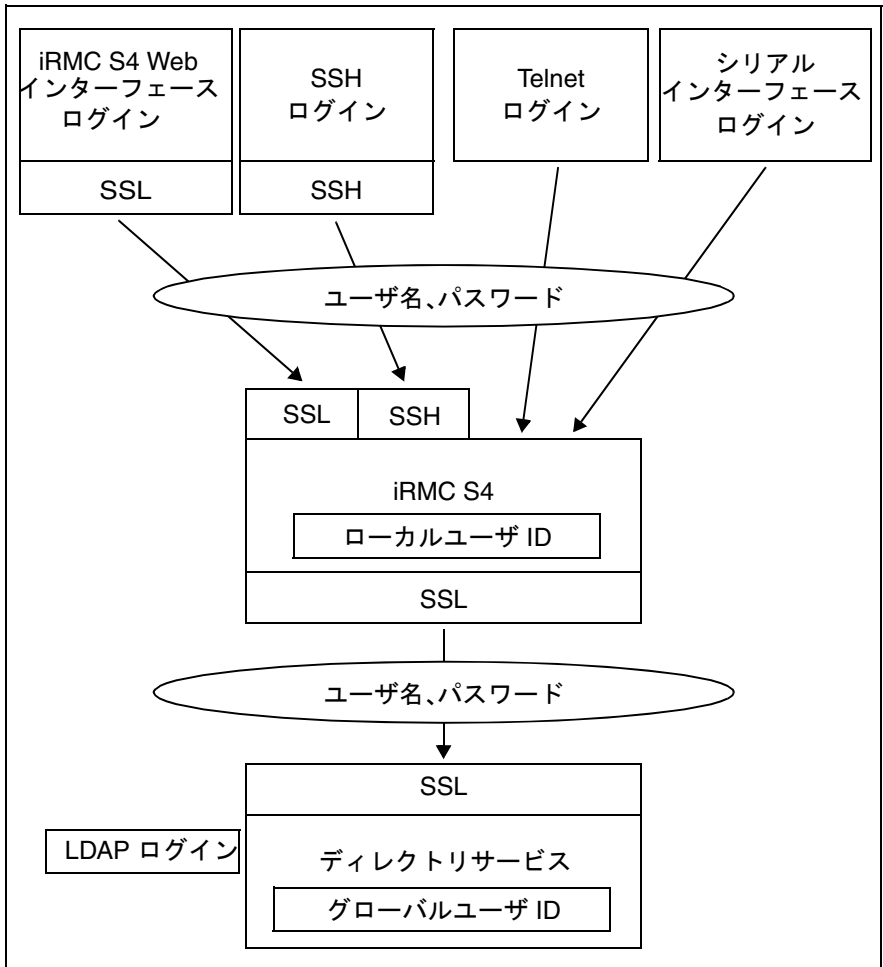



図 64: iRMC S4 経由のログイン認証

iRMC S4 とディレクトリサービスの間の LDAP 接続には、オプションの SSL を使用することを推奨します。SSL で保護された iRMC S4 とディレクトリサービスの間の LDAP 接続では安全なデータ交換が保証されますが、特にユーザ名とパスワードのデータの送信が安全にできます。

iRMC S2/S3 Web インターフェース経由の SSL ログインが必要になるのは、LDAP が有効な場合のみです（「**LDAP 有効化**」オプション、『iRMC S2/S3 - integrated Remote Management Controller』マニュアルを参照）。

8.2 iRMC S4 のグローバルユーザ管理

iRMC S4 のグローバルユーザ ID は、LDAP ディレクトリサービスを利用して集中管理されます。

iRMC S4 ユーザ管理では、現在以下のディレクトリサービスがサポートされます。

– Microsoft® Active Directory
– Novell® eDirectory
– OpenLDAP[OpenLDAP]
– OpenDS / ForgeRock's OpenDJ

この節では次の点について説明します。

– iRMC S4 のグローバルユーザ管理の概略

– LDAP ディレクトリサービスによる iRMC S4 のグローバルユーザ管理の概念

– ディレクトリサービスによるグローバル iRMC S4 ユーザ管理の設定（ディレクトリサービス中で iRMC S4 に特化した許可構造の生成）

– Microsoft Active Directory によるグローバル iRMC S4 ユーザ管理

– Global iRMC S2/S3 によるグローバル iRMC S4 ユーザ管理

– OpenLDAP / OpenDS / OpenDJ によるグローバル iRMC S4 ユーザ管理

i 本節で説明される、ディレクトリサービスのためにユーザが実行する作業とは別に、グローバルユーザ管理には、iRMC S4 上でローカルの LDAP 設定を設定する必要があります。

以下のいずれかの？法でローカル LDAP を設定します。

– iRMC S4 Web インターフェース（『iRMC S4 - integrated Remote Management Controller』マニュアルを参照）

– Server Configuration Manager の使用

なお、次の点に注意してください。

グローバル iRMC S4 ユーザ管理の設定を行うには、使用するディレクトリサービスに関して熟知している必要があります。ディレクトリサービスを熟知した管理者以外は作業を行わないでください。

8.2.1 「概要」

iRMC S4 のグローバルユーザ ID は、ディレクトリサービスのディレクトリにすべてのプラットフォームの分が集中保管されています。これにより、集中サーバによるユーザ ID 管理が可能となっています。そのため、ネットワークでこのサーバに接続されているすべての iRMC S4 で、ユーザ ID を使用することができます。

そのうえ、iRMC S4 のディレクトリサービスを使用することにより、管理対象サーバのオペレーティングシステムに使用されるものと同じユーザ ID を iRMC S4 へのログインにも使用することが可能です。

i グローバルユーザ管理は現在 iRMC S4 の以下の機能ではサポートされていません。

– IPMI-over-LAN 経由のログイン
– SOL 経由のコンソールリダイレクション

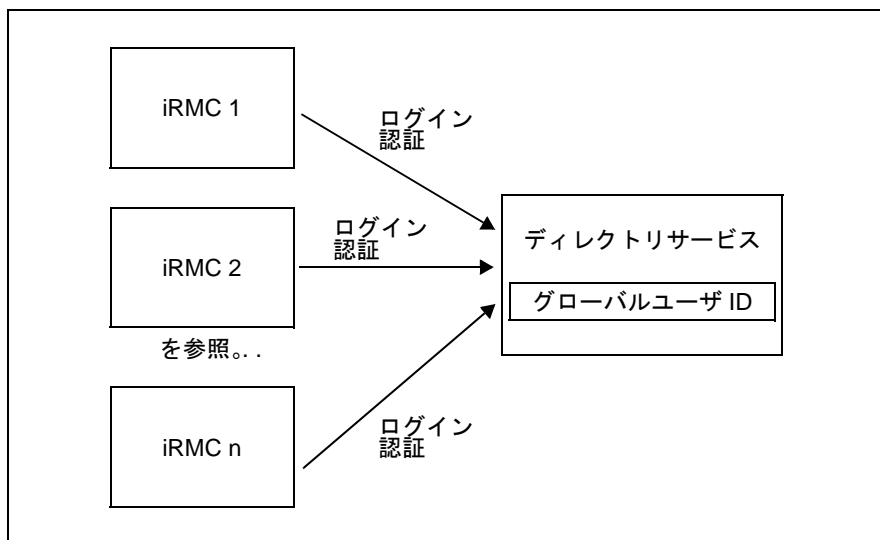



図 65: 複数の iRMC によるグローバルユーザ ID の共用

個々の iRMC S4 と集中ディレクトリサービスの間の通信は TCP/IP プロトコル LDAP （**L**ightweight **D**irectory **A**ccess **P**rotocol）経由で実行されます。LDAP によって、ディレクトリサービスにアクセスする方法が最もよく使われ、ユーザ管理に最も適しています。オプションで、LDAP 経由の通信は、SSL によってセキュリティを確保することができます。

8.2.2 LDAP ディレクトリサービスによる iRMC S4 ユーザの管理 （概念）

> **i** 以下に説明するディレクトリサービスに基づくグローバル iRMC S4 ユーザ管理の概念は、Microsoft Active Directory、Novell eDirectory、OpenLDAP および OpenDS / OpenDJ にも同様に適用されます。図は、Microsoft Active Directory のユーザインターフェースの「**Active Directory ユーザとコンピュータ**」コンソールの例に基づいています。

> **i** 以下の記号は、LDAP 上で文字列を検索するためのメタキャラクタとして予約されています : *, \, &, (,), |, !, =, <, >, ~, :
>
> したがって、ユーザはこれらの文字を相対識別名（RDN）の要素として使用することはできません。

8.2.2.1 役割を使用するグローバル iRMC S4 ユーザ管理

LDAP ディレクトリサーバ経由のグローバル iRMC S4 ユーザ管理では、標準のディレクトリサーバのスキーマを拡張する必要はありません。その代わりに、iRMC S4 に関連するすべての情報は、ユーザ権限も含めて、追加 LDAP グループと組織単位（OU）を使用して提供されます。これらの OU は、LDAP ディレクトリサーバのドメイン内の別々の OU で結合されたものです（228 ページ の図 67 を参照）。

iRMC S4 ユーザは、組織単位（OU）**SVS** で宣言された役割（ユーザ役割）を割り当てられることで、権限を取得します。

ユーザロール（略称 : ロール）による許可の割り当て

iRMC S4（ファームウェアバージョン 3.77 以降）のグローバルユーザ管理では、許可の割り当てをユーザロールにより管理します。この場合は、各ロールは、iRMC S4 上で有効なタスクに基づく許可プロファイルを個々に定義します。

各々のユーザには複数のロールを割り当てることができますので、そのユーザの許可は、割り当てられたロールすべての許可の合計により定義されます。

図 66 は、**Administrator**、**Maintenance**、**Observer** および **UserKVM** の各ロールによるユーザ権限の、ロールに基づく割り当ての概念を図解したものです。

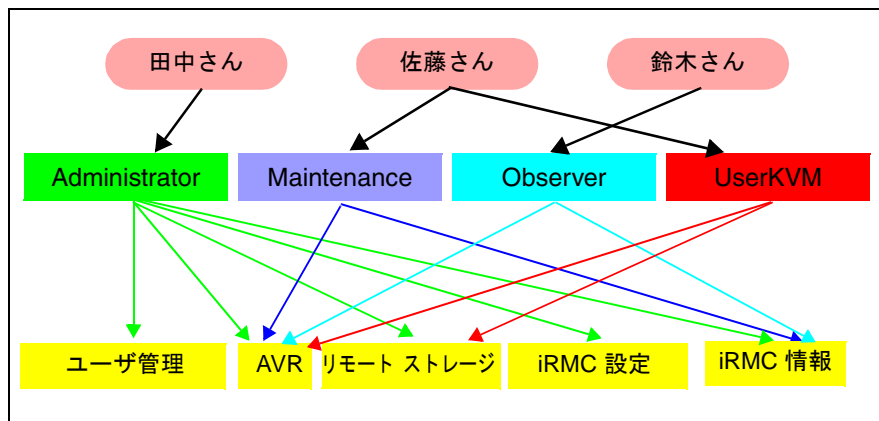



図 66: ロールに基づくユーザ権限の割り当て

ユーザロールの概念には、以下のような重要な利点があります。

– 各々のユーザまたはユーザグループに、個別に許可を割り当てる必要がない。その代わりに、許可はユーザロールに従って割り当てられる。

– 許可のストラクチャが変更になった場合にユーザロールによる許可を適合させるのみでよい。

8.2.2.2 組織単位（OU）SVS

iRMC S4 のファームウェアは、OU **SVS** に保存されている LDAP v2 構造をサポートします。LDAP v2 構造はすべて今後の機能拡張のために設定されています。

「**SVS**」には、OU「**Declarations**」、「**Departments**」および「**User Settings**」が含まれています。

– 「**Declarations**」には、定義されたロールのリストと定義済みの iRMC S4 ユーザ権限のリストが含まれています。

– 「**Departments**」にはユーザ権限のためのグループが含まれています。

– 「**User Settings**」には、メールフォーマット（警告メールに使用します）などのユーザまたはユーザグループ固有の詳細情報と、ユーザシェルのためのグループが含まれています。

i たとえば、Microsoft Active Directory の場合には、iRMC S4 ユーザのエントリは標準 OU である「**Users**」に納められています。ただし、iRMC S4 ユーザは標準ユーザとは異なり、OU「**SVS**」の 1 つまたは複数のグループのメンバーにもなっています。

i **注意事項 :**

ServerView ユーザ管理と iRMC S4 グローバルユーザ管理の両方を同じ組織単位（OU）**SVS** で動作させるには、iRMC S4 ユーザ管理が **DEFAULT** 部門に属するように設定する必要があります。

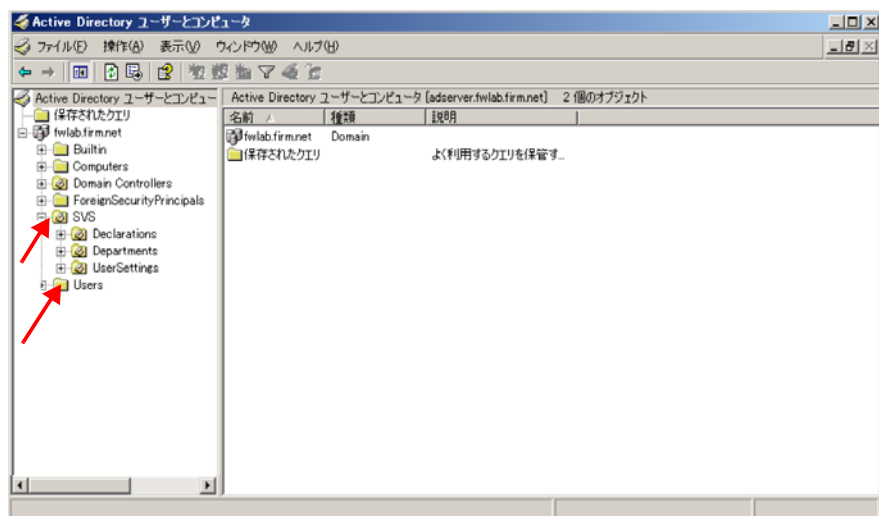



図 67: ドメイン fwlab.firm.net での OU SVS

バージョン 3.6x のファームウェアでは、iRMC S4 用のユーザエントリは基本ドメインの配下のどのポイントにも配置できます。許可グループも基本ドメインの配下のどのポイントにも配置できます。

8.2.2.3 多部門サーバからのアクセス許可

大規模な企業では、iRMC S4 によって管理されるサーバ群は通常さまざまな部門に割り当てられます。その上、管理対象サーバの管理者権限も、多くの場合部門独自の方法で割り当てられます。

注意事項 :

ServerView ユーザ管理と iRMC S4 グローバルユーザ管理の両方を同じ組織単位（OU）**SVS** で動作させるには、iRMC S4 ユーザ管理が **DEFAULT** 部門に属するように設定する必要があります。

部門は「Departments」という OU 内で結合されます

OU「**Departments**」は、iRMC S4 によって管理されるサーバを結合し、多数のグループを形成します。これらは、同じユーザ ID と許可が適用される部門に対応します。たとえば、230 ページ の図 68 では、「**DeptX**」、「**DeptY**」および「**Others**」という部門になります。

「**Others**」というエントリは任意ですが推奨します。「**Others**」は、どの部門にも属さないすべてのサーバを含む、あらかじめ定義された部門名です。「**Departments**」の下にリストされる部門（OU）の数に関しては、制限はありません。

> **i** iRMC S4 でディレクトリサービスを iRMC S4 Web インターフェース（マニュアル『iRMC S4 - integrated Remote Management Controller』を参照）、または Server Configuration Manager を使用して直接サービスを設定する場合は、関連する iRMC S4 が属する管理対象サーバの部門名を指定します。LDAP ディレクトリにその名前の部門がない場合には、「**Others**」部門にある権限を使用します。

230 ページ の図 68 は、**Active Directory ユーザとコンピュータ**を基本としたこのタイプの組織構造の例を表します。

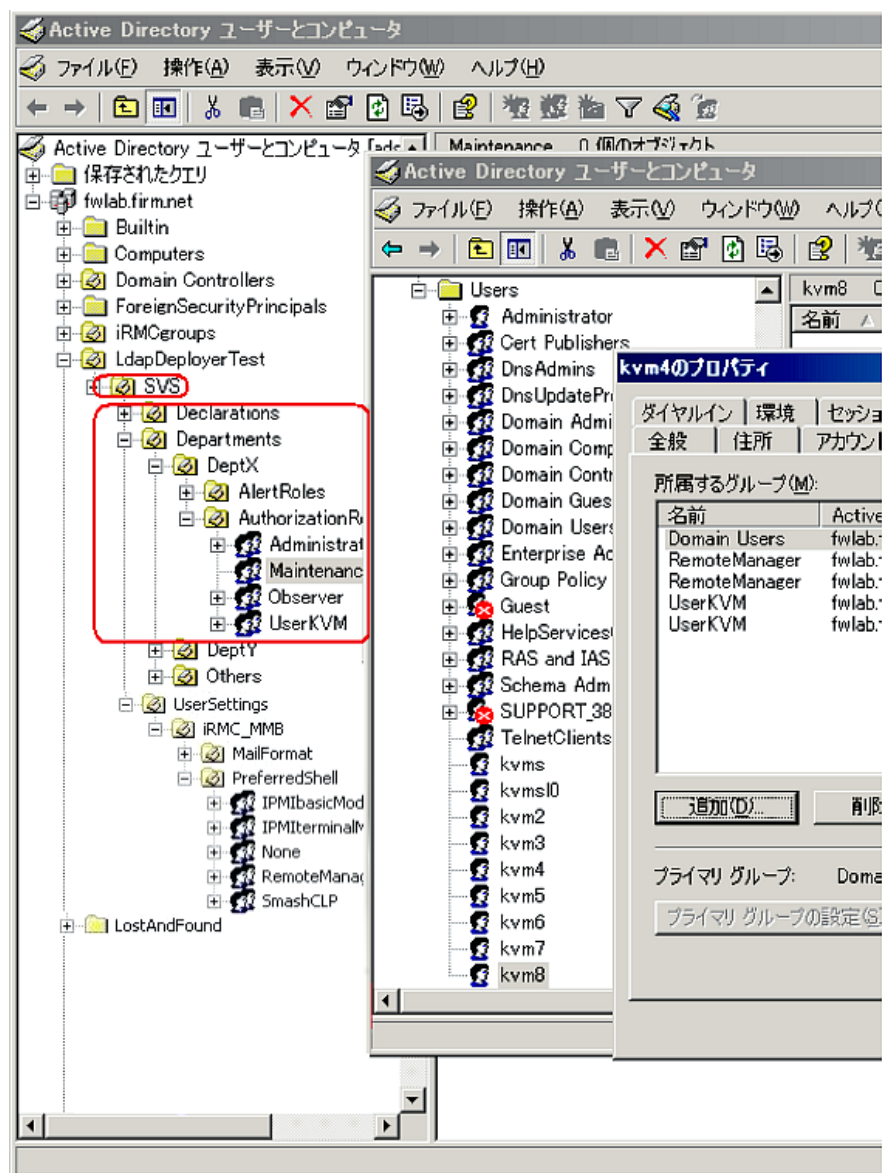



図 68: ドメイン fwlab.firm.net の組織構造

8.2.2.4 SVS: 許可プロファイルはロールにより定義される

要求される関連ユーザロール（認証ロール）は各部門の直下にリストされます（230 ページ の図 68）。ここにリストされるロールはすべて OU「**Declarations**」で定義されます。それ以外にロールの数に関する制限はありません。ロールの名前は必要に応じて選ぶことができますが、運用するディレクトリサービスに賦課された特定のシンタックス要件に合わなければなりません。各認証ロールは、iRMC S4 上の処理のためにタスクに基づく許可プロファイルを個々に定義します。

> **i** 認証ロールと同様に警告ロールもリストされます。各警告ロールには Email で警告するための固有の警告プロファイルを定義します（289 ページ の「グローバル iRMC S4 ユーザ宛ての Email 警告の設定」の項を参照）。

ユーザロールの表示

「**Active Directory ユーザとコンピュータ**」のストラクチャツリー（図 69 を参照）の「**SVS**」の配下にある部門（たとえば **DeptX**）を選択し（1）、関連するノード「**DeptX – Authorization Roles**」を展開すると、そこに定義されたユーザ役割（ここでは **DeptX**）が表示されます（2）。

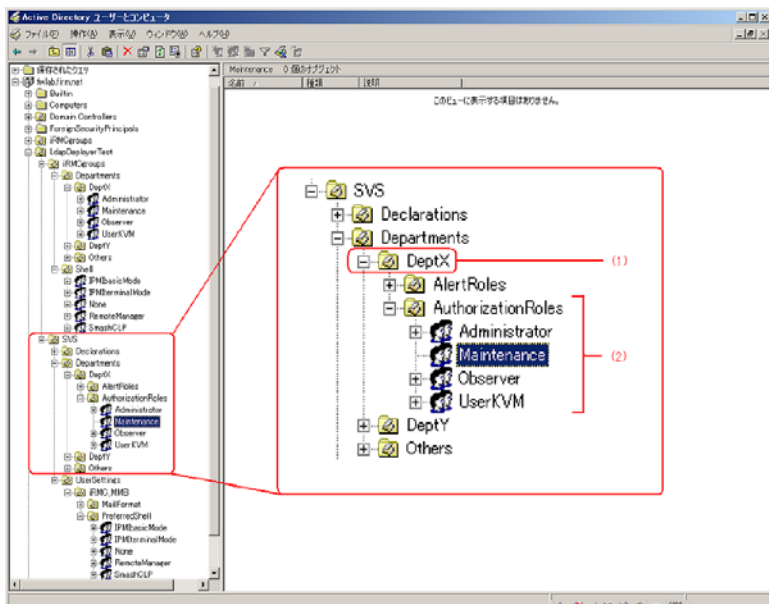



図 69: 「ユーザとコンピュータ」スナップインの中のユーザロールの表示

ユーザがメンバーとなっている Active Directory フォルダの表示

「Active Directory ユーザとコンピュータ」のストラクチャツリーの**「Users」**の配下にあるユーザ（**kvms4** など）を選択して（図 70 を参照）（1）、コンテキストメニューから**「プロパティ」-「所属するグループ」**を選択してこのユーザの「**プロパティ**」ダイアログボックスを開いた場合、ユーザが属する権限グループ（ここでは **kvms4**）が「**所属するグループ**」タブに表示されます（2）。

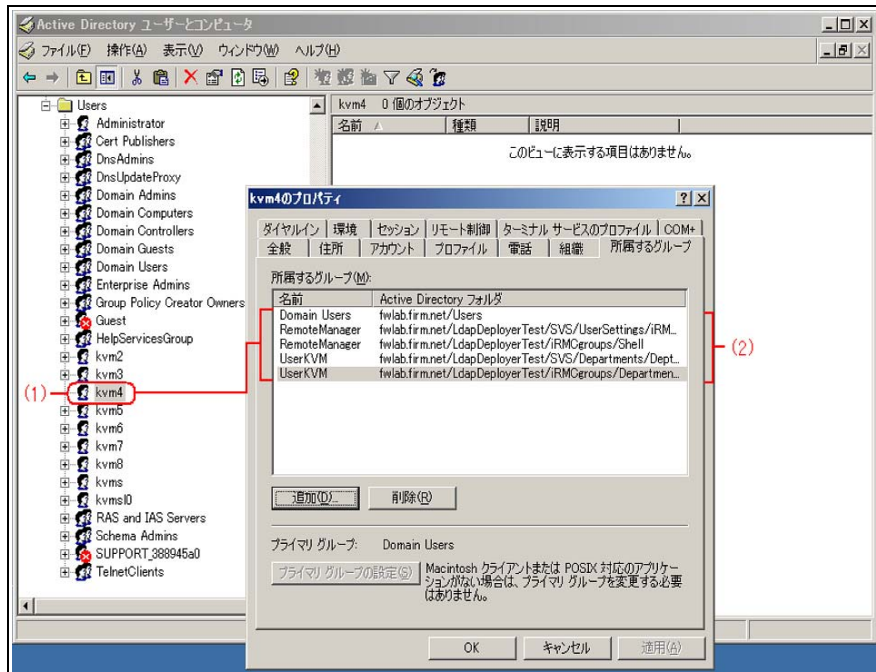



図 70: ユーザ「kvms4」のプロパティダイアログボックス

8.2.3 SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除

ディレクトリサービスを使用してグローバル iRMC S4 ユーザ管理を操作できるようにするために、LDAP ディレクトリに「**SVS**」ストラクチャ（OU）を作成する必要があります。

「**SVS**」ストラクチャの生成または変更には **SVS_LdapDeployer** を使用します。「**SVS_LdapDeployer**」は Java アーカイブ（「**SVS_LdapDeployer.jar**」）ですが、ServerView Suite の DVD に収録されています。

この節では以下について説明します。

– 「**SVS_LdapDeployer**」の設定ファイル

– **SVS_LdapDeployer**

– 「**SVS_LdapDeployer**」のコマンドとオプション

– 一般的な使用例

8.2.3.1 設定ファイル（XML file）

「**SVS_LdapDeployer**」は **XML** 設定ファイルに基づいて LDAP ストラクチャを生成します。この入力ファイルには、ストラクチャ「**SVS**」の XML 構文によるストラクチャ情報が含まれています。

i 設定ファイルの構文については、サンプル設定ファイル「**Generic_Settings.xml**」および「**Generic_InitialDeploy.xml** 」で説明されています。これらのファイルは、ServerView Suite DVD に収録される **jar** アーカイブ「**SVS_LdapDeployer.jar** 」の中にあります。

i ディレクトリサーバ接続のための有効な接続データはかならず <Settings> 入力ファイルの下に入力しなければなりません。

サーバにアクセスするための認証データは任意で入力することができます。あるいは、「**SVS_LdapDeloyer**」のコマンドラインで認証データを指定することもできます。

「**SVS_LdapDeployer**」を呼び出すときに設定ファイルまたはコマンドラインで認証データを指定しないと、「**SVS_LdapDeployer**」から認証データをランタイムで入力するように求められます。

8.2.3.2 SVS_LdapDeployer の起動

以下の手順に従って、**SVS_LdapDeployer** を起動します。

▶ Java アーカイブ（**jar** アーカイブ）の「**SVS_LdapDeployer.jar**」をディレクトリサーバ上のフォルダに保存します。

▶ ディレクトリサーバのコマンドインターフェースを開きます。

▶ **jar** アーカイブ「**SVS_LdapDeployer.jar**」が保存されているフォルダに移動します。

▶ 次の構文を使用して「**SVS_LdapDeployer**」を呼び出します。

```
java -jar SVS_LdapDeployer.jar <command> <file>
                                              [<option>...]
```

i 「**SVS_LdapDeployer**」の実行中に行われるさまざまな手順が通知されます。詳細な情報は **log.txt** ファイルで見ることができます。このファイルは「**SVS_LdapDeployer**」実行時に毎回実行フォルダの中に作られます。

i 以下では、「LDAPv1 ストラクチャ」と「LDAPv2 ストラクチャ」は、認証データの ServerView 固有の設定レイアウトを示すために使用され、LDAP プロトコルのバージョン 1 および 2 を指すものではありません。

i **-import** と **-sychronize** コマンド（以下を参照）は、LDAPv1 ストラクチャ（ファームウェアバージョン 3.77 未満搭載の iRMC S2 と iRMC）の場合にのみ必要です。詳細については、マニュアルを参照してください。

– 『iRMC S2 - integrated Remote Management Controller』、2011 年 5 月以前の版

– 「iRMC - integrated Remote Management Controller」。

<command>

実行する処理を指定します。

以下のコマンドを使用可能です。

-deploy

グローバル iRMC S4 ユーザ管理の LDAP ストラクチャをディレクトリサーバの中に作成します（236 ページを参照）。

-delete

グローバル iRMC S4 ユーザ管理に用いた LDAP ストラクチャをディレクトリサーバから削除します（238 ページを参照）。

-import

既存の LDAP v1 ストラクチャから 同等の LDAP v2 ストラクチャを作成します。

-synchronize

LDAP v2 に何らかの変更を行うと、その変更を反映して既存の LDAP v1 ストラクチャを同じように変更します。

<file>

「**SVS_LdapDeploy**」が入力ファイルとして用いる設定ファイル（**.xml**）。この設定ファイルには、**SVS** ストラクチャのストラクチャ情報が **XML** 構文で含まれています。

> i 設定ファイルの構文については、サンプル設定ファイル「**Generic_Settings.xml**」および「**Generic_InitialDeploy.xml** 」で説明されています。これらのファイルは、ServerView Suite DVD に収録される **jar** アーカイブ「**SVS_LdapDeployer.jar** 」の中にあります。

<option> [<option> ...]

指定されたコマンドの実行をコントロールするためのオプションです。

これ以降の項では、「**SVS_LdapDeployer**」で使用できる個々のコマンドを関連するオプションと合わせて詳しく解説します。

> i 「**SVS_LdapDeployer**」は、すべてのグループが含まれる必要なサブツリーを生成しますが、ユーザとグループの関連付けはしません。
>
> ユーザエントリは、ディレクトリサービスで OU「**SVS**」か「iRMCgroups」または双方を生成した後、運用するディレクトリサービスの適切なツールを使用して作成し、グループに割り当てます。

8.2.3.3 -deploy: LDAP v2 ストラクチャの作成と変更

-deploy コマンドを使用して、ディレクトリサーバ上に新しい LDAP ストラクチャを作成したり、既存の LDAP ストラクチャに新しいエントリを追加したりすることができます。

既存の LDAP ストラクチャからエントリを削除する場合は、まず **-delete** コマンド（238 ページを参照）を使用して LDAP ストラクチャ自体を削除し、次に適切に修正した設定ファイルを使用して LDAP ストラクチャを再作成する必要があります。

構文：

```
-deploy <file> [-structure {v1 | v2 | both}]
      [ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

設定データを含む **XML** ファイル。

設定ファイルの <Data> 部にはストラクチャを最初に生成するため、または展開するために必要なロールと部門がすべて含まれなければなりません。

-structure v1 | -structure v2 | -structure both

LDAP v1 ストラクチャまたは、LDAP v2 ストラクチャ、あるいは、LDAP v1 と LDAP v2 両方のストラクチャを作成します。

iRMC S4 のユーザ管理には、常に LDAP v2 ストラクチャが必要です。

-username <user>

ディレクトリサーバにログインするためのユーザ名です。

-password <password>

ユーザ <user> のパスワード。

-store_pwd

-deploy が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルトでは、ランダムに生成された鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保存してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザもアクセスできる場合は、オプション **-kloc** および **-kpwd** を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。
<password> が指定されない場合は、現行のランタイムのスナップショットを基にしてパスワードが自動的に生成されます。

8.2.3.4 -delete : LDAPv2 ストラクチャの削除

-delete コマンドを使用して、ディレクトリサーバから LDAP v2 ストラクチャを削除することができます。

構文：

```
-delete <file> [-structure {v1 | v2 | both}]
      [ -username <user>]
      [ -password <password>][ -store_pwd <path>][ -kloc <path>]
      [ -kpwd [<key-password>]]
```

<file>

削除するストラクチャを指定する **XML** ファイルです。

-structure v1 **|** -structure v2 **|** -structure both

LDAP v1 ストラクチャまたは、LDAP v2 ストラクチャ、あるいは、LDAP v1 と LDAP v2 両方のストラクチャを削除します。

iRMC S4 には、常に LDAP v2 ストラクチャが必要です。

-username <user>

ディレクトリサーバにログインするためのユーザ名です。

-password <password>

ユーザ <user> のパスワード。

-stor_pwd

-delete が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルにその暗号化されたパスワードを保存します。デフォルトでは、ランダムに生成された鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

注意！

ランダムに生成された鍵は安全な場所に保存してください。既定のターゲットフォルダがセキュリティの面で適切でない場合、または鍵が保管されたフォルダに他のユーザもアクセスできる場合は、オプション **kloc** および **-kpwd** を使用して、鍵を安全に保管してください。

-kloc <path>

ランダムに生成された鍵を <path> の下に保存します。
このオプションが指定されない場合は、鍵は「**SVS_LdapDeployer**」が実行されるフォルダに保管されます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。<password> が指定されない場合は、現行のランタイムのスナップショットを基にしてパスワードが自動的に生成されます。

8.2.4 一般的な使用例

「**SVS_LdapDeployer**」を使用する際の一般的な使用例を、以下に示します。

8.2.4.1 LDAP v2 ストラクチャの初期設定の実行

iRMC S4（ファームウェア 3.77 以降）のグローバルユーザ管理を初めて設定する場合、LDAP v2 のストラクチャが必要となります。

推奨する方法：

LDAP v2 ストラクチャの部門定義を生成します（**SVS**）。

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure v2
```

8.2.4.2 LDAP v2 ストラクチャの再生成と展開

LDAP v2 ストラクチャを再生成するか、既存の LDAP v2 ストラクチャを展開したい場合。

推奨する方法：

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -structure -structure v2
```

または

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
```

8.2.4.3 LDAP v2 ストラクチャの再生成と、認証データの要求と保存

LDAP v2 ストラクチャを再生成したい場合。認証データはコマンドラインを用いて作成し、保存します。

推奨する方法：

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
     -store_pwd -username admin -password admin
```

i ログインデータを保存した後には、ユーザ名およびパスワードを指定せずに「**SVS_LdapDeployer**」を使用してディレクトリサーバに接続できます。その際、使用可能な数値が XML 設定ファイルに保存されている場合は、「**SVS_LdapDeployer**」はその数値を使用します。「**SVS_LdapDeployer**」が保存されたパスワードを使用できるのは、暗号化されたパスワードを解読できる場合のみです。そのため、「**SVS_LdapDeployer**」を、「**-store_pwd**」オプション（237 ページを参照）を用いた前の呼び出しで適用したのと同じランタイム環境で実行する必要があります。このコンテキストで言う「同じランタイム環境」とは、「同じコンピュータを使用する同じユーザ」または「鍵が保存されているフォルダにアクセスする許可を持つユーザ（**-kloc** オプション、237 ページを参照）」を意味します。

i 今後は、「**SVS_LdapDeployer**」を呼び出すときに、すでに保存してあるユーザアカウントを使用することもできます。さらに、データをコマンドラインに明確に指定するか、「**SVS_LdapDeployer**」がそのように要求する場合には、他の認証データを一時的に使用することもできます。

8.2.5 Microsoft Active Directory による iRMC S4 ユーザ管理

この項では、iRMC S4 ユーザ管理を Microsoft Active Directory に統合する方法を説明します。

前提条件：

LDAP v2 ストラクチャまたはそのいずれかが Active Directory サービスの中に生成されていること（233 ページ の「SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除」の項を参照）。

以下の手順を実行して、iRMC S4 ユーザ管理を Microsoft Active Directory に統合します。

1. Active Directory サーバ上の iRMC S4 LDAP/SSL アクセスを設定します。
2. iRMC S4 のユーザを Active Directory の iRMC S4 ユーザグループに割り当てます。

8.2.5.1 Active Directory サーバ上の iRMC S4 LDAP/SSL アクセスを設定します。

iRMC S4-LDAP の統合には、OpenSSL プロジェクトに基づき Eric Young 氏が開発した SSL 実装を使用します。SSL copyright の複製リストを 296 ページ に掲載します。

iRMC S4 が SSL 経由で LDAP を使用できるようにするには、RSA 証明書が必要です。

LDAP アクセスを設定する手順は以下の通りです。

1. 企業 CA をインストールします。
2. ドメインコントローラ用の RSA 証明書を生成します。
3. RSA 証明書をサーバにインストールします。

企業 CA のインストール

CA は「認証局」です。企業 CA（認証局）はドメインコントローラ自体または別のサーバにインストールすることができます。

ディレクトリサーバをドメインコントローラに直接インストールするほうが、別のサーバにインストールするよりも必要な手順が少ないので簡単です。

企業 CA をドメインコントローラ以外のサーバにインストールする方法を、以下に説明します。

企業 CA をインストールして正しく設定するには、Active Directory 環境とインストール済みの IIS（**I**nternet **I**nformation **S**ervices）が必要です。

企業 CA のインストールは以下の手順で行います。

► Windows のスタートメニューで、次のように進みます。

「スタート」-「コントロールパネル」-「プログラムの追加と削除」-「Windows コンポーネントの追加と削除」

► Windows コンポーネントのウィザードで、「**Components**」から「**Certificate Services**」を選択します。

► 「**Certificate Services**」をダブルクリックし、「**Certificate Services Web Enrollment Support**」と「**Certificate Services CA**」のオプションが選択されていることを確認します。

► 「**Enterprise root CA**」を選択します。

- オプション「**Use custom settings to generate the key pair and CA certificate**」を選択します。
- 「**Microsoft Base DSS Cryptographic Provider**」を選択して長さ 1024 バイトの DSA 証明書を作成します。
- 公開認証局証明書（CA 証明書）をエクスポートします。

  これは次の手順で行います。

  - Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させせます。
  - ローカルコンピュータ証明書のスナップインを追加します。
  - **「Certificates（Local Computer）」-「Trusted Root Certification Authorities」-「Certificates」**へと進み、ダブルクリックします。
  - 新規に作成された認証局からの証明書をダブルクリックします。
  - 証明書ウィンドウの「**Details**」タブをクリックします。
  - 「**Copy to File**」をクリックします。
  - 認証局証明書のファイル名を選び、「**Finish**」をクリックします。
- 公開認証局証明書をドメインコントローラ上の証明書ディレクトリ **Trusted Root Certification Authorities** にロードします。

  これは次の手順で行います。

  - 認証局証明書を収めたファイルをドメインコントローラに転送します。
  - Windows エクスプローラーで、新規に作成された認証局からの証明書を開きます。
  - 「**Install Certificate**」をクリックします。
  - 「**Place all certificates in the following store**」の下の「**Browse**」をクリックし、「**Trusted Root Certification Authorities**」を選択します。
  - Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させせます。
  - ローカルコンピュータ証明書のスナップインを追加します。
  - 現在のユーザの証明書のスナップインを追加します。
  - 認証局証明書（CA 証明書）を、現在のユーザの **Trusted Root Certification Authorities** ディレクトリからローカルコンピュータの **Trusted Root Certification Authorities** にコピーします。

ドメインコントローラ証明書の作成

ドメインコントローラの RSA 証明書の作成は、以下の手順で行います。

► 下記の内容の **request.inf** という名前のファイルを作成します。

[Version]
Signature="$Windows NT$"[NewRequest]
Subject = "CN=<full path of domain controller host>"
KeySpec = 1
KeyLength = 1024
Exportable = TRUE
MachineKeySet = TRUE
SMIME = FALSE
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

RequestType = PKCS10
OID=1.3.6.1.5.5.7.3.1
; サーバ認証用

► ファイル **request.inf** で、「Subject=」の下の指定を、用いているドメインコントローラの名前に合わせます（例：
`Subject = “CN=domino.fwlab.firm.net”`。

► Windows のプロンプトウィンドウに、「**certreq -new request.inf request.req**」と入力します。

► 認証局ブラウザに次の URL を入力します：
http://localhost/certsrv

► 「**Request a Certificate**」をクリックします。

► 「**advanced certificate request**」をクリックします。

► 「**Submit a certificate request**」をクリックします。

► ファイル **request.req** の内容を「**Saved Request**」ウィンドウにコピーします。

► 「**Web Server**」証明書のテンプレートを選択します。

► 証明書をダウンロードして、ファイル **request.cer** などに保存します。

- Windows のプロンプトウィンドウに、「**certreq -accept request.cer**」と入力します。
- 証明書を秘密鍵付きでエクスポートします。

  これは次の手順で行います。

  - Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させます。
  - ローカルコンピュータ証明書のスナップインを追加します。
  - 以下の順に移動します。
「Certificates（Local Computer）」-「Personal Certificates」-「Certificates」
  - 新規サーバ認証局証明書をクリックします。
  - 証明書ウィンドウの「**Details**」タブをクリックします。
  - 「**Copy to File**」をクリックします。
  - 「**Yes, export the private key**」を選択します。
  - パスワードを割り当てます。
  - 証明書のファイル名を選び、「**Finish**」をクリックします。

ドメインコントローラ証明書のサーバへのインストール

ドメインコントローラ証明書のサーバへのインストールは、次の手順で行います。

- ► 作成されたばかりのドメインコントローラ証明書のファイルをドメインコントローラにコピーします。
- ► ドメインコントローラ証明書をダブルクリックします。
- ► 「**Install Certificate**」をクリックします。
- ► 証明書をエクスポートするときに割り当てたパスワードを使用します。
- ► 「**Place all certificates in the following store**」の下の「**Browse**」をクリックし、「**Personal Certificates**」を選択します。
- ► Windows のプロンプトウィンドウで「**mmc**」と入力して、Management Console を起動させます。
- ► ローカルコンピュータ証明書のスナップインを追加します。
- ► 現在のユーザの証明書のスナップインを追加します。
- ► ドメインコントローラ証明書を現在のユーザの **Personal Certificates** ディレクトリからローカルコンピュータの **Personal Certificates** ディレクトリにコピーします。

8.2.5.2 iRMC S4 ユーザへのユーザロールの割り当て

iRMC S4 ユーザにユーザロール（認証ロール）を以下の方法で割り当てることができます。

– ユーザエントリに基づいて
– または、ロールエントリ / グループエントリ

以下の例では、LDAP v2 ストラクチャを使用して、OU「**SVS**」のロールエントリに基づく割り当てを説明しています。

ユーザエントリに基づく割り当て方法もほぼ同じです。

Active Directory にユーザを手作業で入力する必要があります。

次の手順に従います。

► スナップイン「**Active Directory ユーザとコンピュータ**」を開きます。

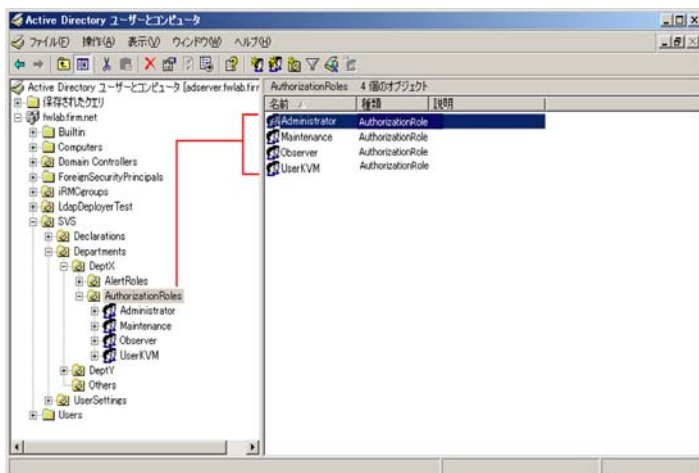



図 71: スナップイン「Active Directory ユーザとコンピュータ」

► 認証ロールをダブルクリックします（ここでは Administrator）。

「**Administrator のプロパティ**」ダイアログが開きます（248 ページ の 図 72 を参照）。

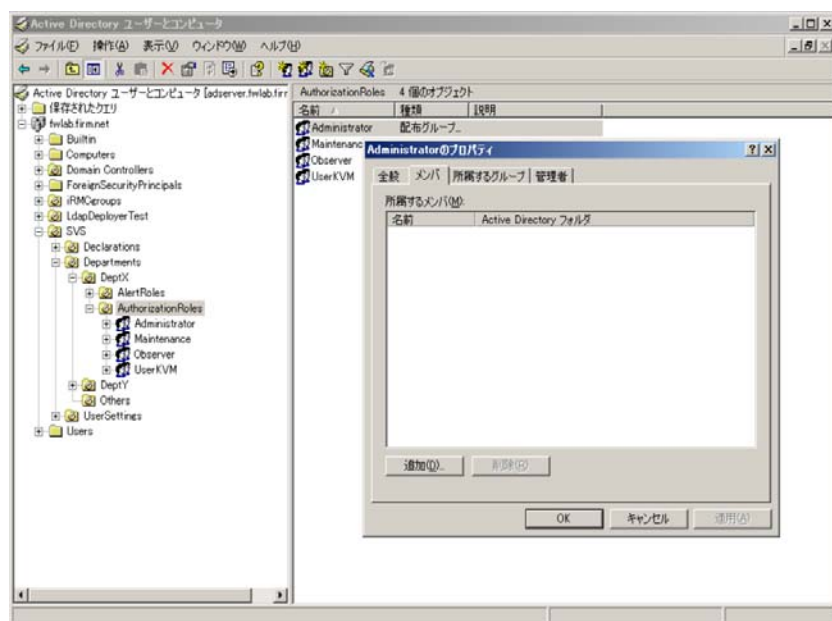



図 72: 「Administrator のプロパティ」ダイアログ

► 「**メンバ**」タブを選択します。

► 「**追加**」をクリックします。ボタンをクリックします。

「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログが開きます（248 ページ の図 73 を参照）。

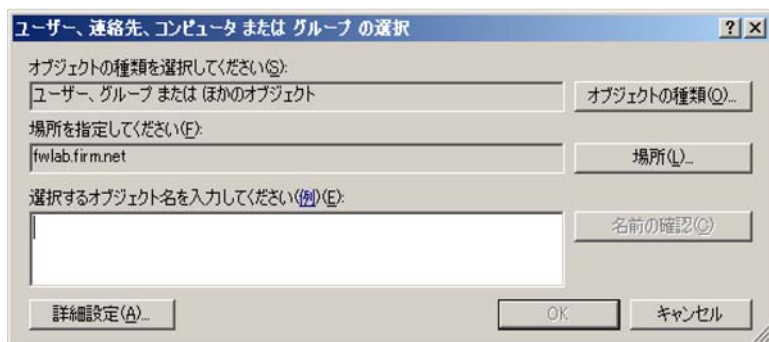



図 73: 「ユーザ、連絡先、コンピュータ または グループの選択」ダイアログ

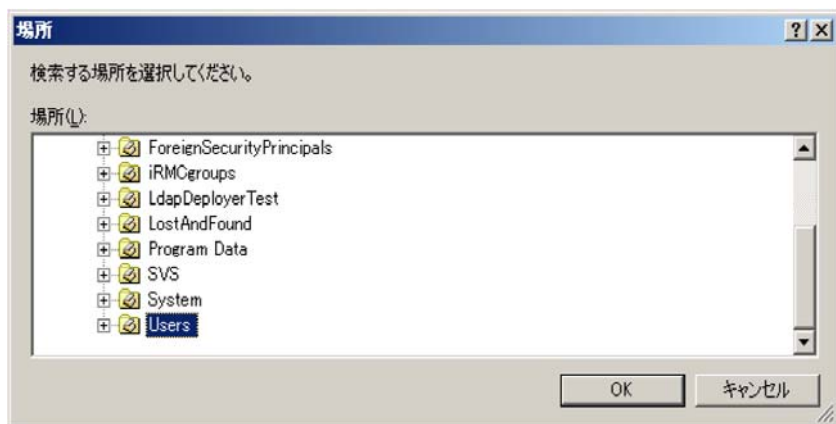
► 「**場所**」をクリックします。ボタンをクリックします。

「**場所**」ダイアログが開きます。

図 74: 「場所」ダイアログ

► 該当するユーザを含むコンテナ（OU）を選択します。（デフォルト値は OU「**Users**」となります）。「**OK**」をクリックして確定します。

「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログが開きます（249 ページ の図 75 を参照）。

ディレクトリ内の他の位置にユーザを ?? することもできます。

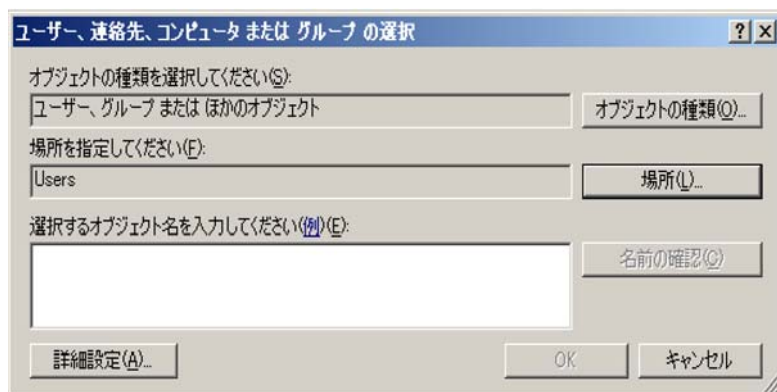



図 75: 「ユーザ、連絡先、コンピュータ または グループの選択」ダイアログ

▶ 「**詳細設定**」をクリックします。ボタンをクリックします。

「**ユーザ、連絡先、コンピュータまたはグループの選択**」ダイアログが展開されます（250 ページ の図 76 を参照）。

図 76: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ ? 検索画面

▶ 「**今すぐ検索**」ボタンをクリックしてドメイン内のすべてのユーザを表示させます。

「**検索結果**」の表示部に検索結果が表示されます（251 ページ の図 77 を参照）。

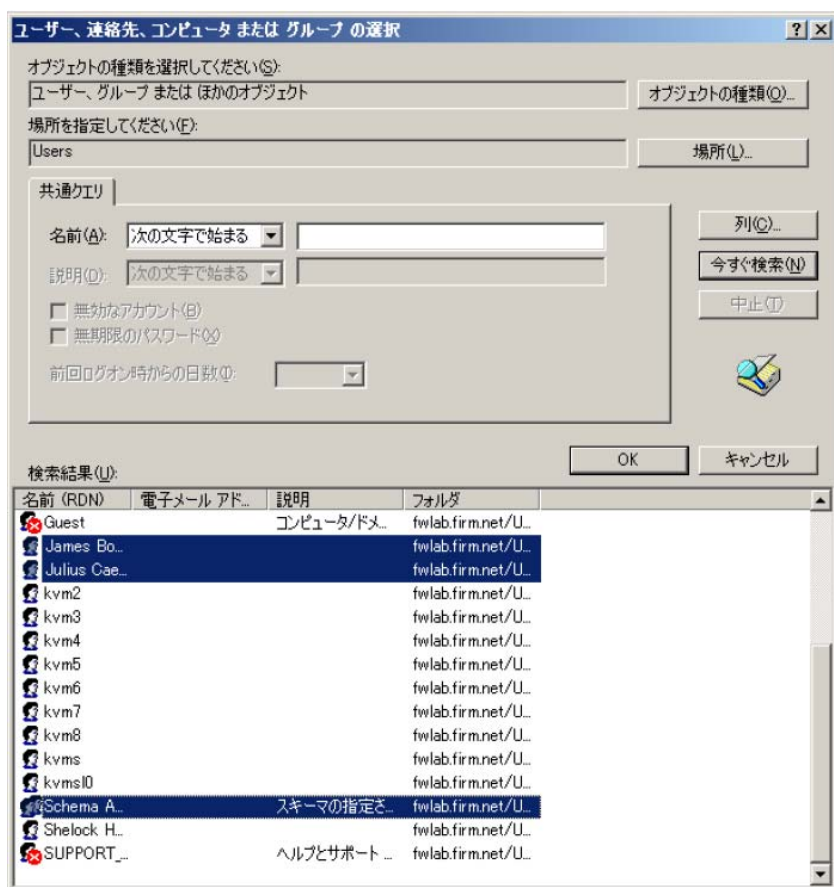



図 77: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ ? 検索結果表示

► グループに追加するユーザを選択し、「**OK**」をクリックして確定します。

選択したユーザが表示されます（252 ページ の図 78 を参照）。

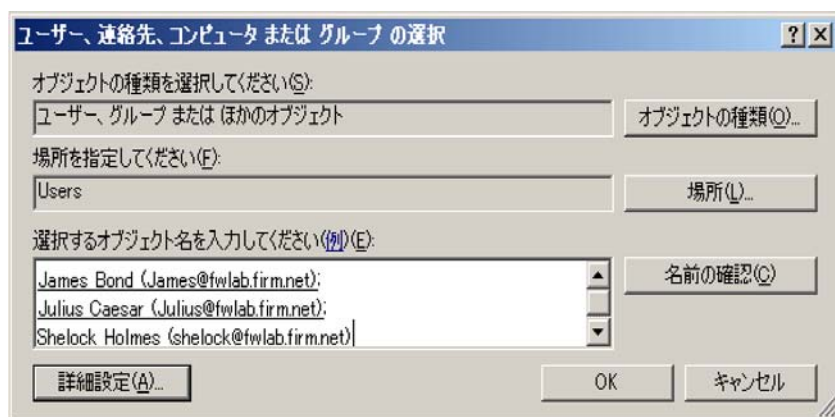



図 78: 「ユーザ、連絡先、コンピュータまたはグループの選択」ダイアログ ? 検索結果確認

► 「**OK**」をクリックして確定します。

8.2.6 Novell eDirectory によるグローバル iRMC S4 ユーザ管理

この節では次の点について説明します。

– Novell eDirectory システムのコンポーネントとシステム要件

– Novell eDirectory のインストール

– Novell eDirectory の設定

– iRMC S4 ユーザ管理の Novell eDirectory への統合

– Novell eDirectory 管理のためのヒント

> **i** 以下に Novell _eDirectory のインストールと設定を詳しく説明します。eDirectory についての広範な知識は必要ありません。すでに Novell eDirectory に習熟しているユーザは、初めの 3 つの節を飛ばして 267 ページ の「iRMC S2/S3 ユーザ管理の Novell eDirectory への統合」の項 に進んでください。

8.2.6.1 ソフトウェアコンポーネントとシステム要件

> **i** 以下にリストされた指定されたバージョン以降のコンポーネントを使用してくださ い。

Novell eDirectory（以前の NDS）は次のソフトウェアコンポーネントで構成されています。

– eDirectory 8.8 : **20060526_0800_Linux_88-SP1_FINAL.tar.gz**

– eDirectory 8.8 : **eDir_88_iMan26_Plugins.npm**

– iManager: SuSE の場合は **iMan_26_linux_64.tgz**、それ以外は **iMan_26_linux_32.tgz**

– ConsoleOne : **c1_136f-linux.tar.gz**

Novell eDirectory をインストールし運用するには、以下のシステム要件を満たす必要があります。

– OpenSSL をインストールする必要があります。

  > **i** OpenSSL がインストール済みでない場合、
  >
  > ► OpenSSL をインストールしてから、Novell eDirectory のインストールを開始してください。

– 512 MB の RAM の空き領域

8.2.6.2 Novell eDirectory のインストール

Novell eDirectory をインストールするには、下記のコンポーネントをインストールする必要があります。

– eDirectory Server および管理ユーティリティ

– iManager（管理ユーティリティ）

– ConsoleOne（管理ユーティリティ）

Novell eDirectory インストールの前提条件：

– Linux サーバ OS のフルインストールと稼動。

– ファイヤーウォールを次のポートに接続可能な設定にします：8080, 8443, 9009, 81, 389, 636。

OpenSuSE では、ファイル **/etc/sysconfig/SuSEfirewall2** の中でこの設定を行います。

► ファイル **/etc/sysconfig/SuSEfirewall2** に、エントリ「**FW_SERVICES_EXT_TCP**」を次のように追加します。

```
FW_SERVICES_EXT_TCP="8080 8443 9009 81 389 636"
```

– eDirectory インストールガイドに従ってシステムにマルチキャストルーティングの設定を行います。

SuSE Linux の場合は以下の通り進めてください。

► ファイル **/etc/sysconfig/network/ifroute-eth0** を作成するか、（作成済みの場合は）開いてください。

► **/etc/sysconfig/network/ifroute-eth0** に以下の行を追加します。

```
224.0.0.0  0.0.0.0  240.0.0.0  eth0
```

この操作で *eth0* がシステム構成に取り込まれます。

eDirectory Server、eDirectory ユーティリティ、iManager および ConsoleOne インストールの前提条件：

– インストールを実行するにはルート権限が必要です。

– 以下の手順でインストールを実行する前に、必要なすべてのファイルをディレクトリ（たとえば **/home/eDirectory**）にコピーしておく必要があります。必要なファイルは以下のとおりです。

20060526_0800_Linux_88-SP1_FINAL.tar.gz
iMan_26_linux_64.tgz
c1_136f-linux.tar.gz

eDirectory Server と管理ユーティリティのインストール

次の手順に従います。

► ルート権限（スーパーユーザ）でログインします。

► インストールに必要なファイルを含むディレクトリに移動します（この例では **/home/eDirectory**）。

```
cd /home/eDirectory
```

► **20060526_0800_Linux_88-SP1_FINAL.tar.gz** アーカイブを解凍します。

```
tar -xzvf 20060526_0800_Linux_88-SP1_FINAL.tar.gz
```

解凍すると、**/home/eDirectory** に **eDirectory** という新しいサブディレクトリが作られます。

eDirectory Server のインストール

► このディレクトリ **eDirectory** のサブディレクトリ **setup** に進みます。

```
cd eDirectory/setup
```

► インストール用スクリプト **./nds-install** を呼び出します。

```
./nds-install
```

► 「y」を入力して EULA を承認し、[Enter] キーで確定します。

► どのプログラムをインストールするか尋ねられたら、

「**install the Novell eDirectory server**」に「1」を入力し、[Enter] キーで確定します。

これで、eDirectory パッケージがインストールされます。

Novell eDirectory Server がインストールできたら、eDirectory までのパス名を環境変数で更新し、これらの変数をエクスポートします。

► この操作を行うには、設定ファイル（この例では「**/etc/bash.bashrc**」）を開き、次の行を指定された順序で「# End of ...」の前に入力します。

```
export PATH/opt/novell/eDirectory/bin:/opt/novell/eDirectory/
       sbin:$PATH

export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib:/
       opt/novell/eDirectory/lib/nds-modules:/opt/novell/
       lib:$LD_LIBRARY_PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/
       man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/
       locale:$TEXTDOMAINDIR
```

► ターミナルを閉じ、新しいターミナルを立ち上げて環境変数をエクスポートします。

eDirectory 管理ユーティリティのインストール

► ディレクトリ **eDirectory** のサブディレクトリ **setup** に移動します。

```
cd eDirectory/setup
```

► インストール用スクリプトを呼び出します。

```
./nds-install
```

► 「y」を入力して EULA を承認し、[Enter] キーで確定します。

► どのプログラムをインストールするか尋ねられたら、

「**install the Novell eDirectory adminsitration utilities**」に「2」を入力し、[Enter] キーで確定します。

これで、eDirectory 管理ユーティリティがインストールされます。

iManager のインストールと起動

Novell eDirectory のインストールには iManager を使用することを推奨します。SLES10 または OpenSuSE にインポートする場合は、アーカイブ ***_64.tgz** を使用します。

次の手順に従います。

- ルート権限（スーパーユーザ）でログインします。
- ディレクトリ **/home/eDirectory** に移動します。

```
cd /home/eDirectory
```

- アーカイブ **iMan_26_linux_64.tgz** を解凍します。

```
tar -xzvf iMan_26_linux_64.tgz
```

解凍すると、**/home/eDirectory** に **iManager** という新しいサブディレクトリが作られます。

- **iManager** の **installs** サブディレクトリに進みます。

```
cd iManager/installs/linux
```

- インストール用スクリプトを呼び出します。

```
./iManagerInstallLinux.bin
```

- インストール時のメッセージを出力する言語を選択します。
- クリックを繰り返し、EULA を承認します。
- 「**1- Novell iManager 2.6, Tomcat, JVM**」を選択して iManager をインストールします。
- 「**1- Yes**」を選択してプラグインをダウンロードします。
- ダウンロードにデフォルトのパスを使う場合は [Enter] キーを押します。

インストールプログラムがインターネット上でダウンロードするサイトを検索します。この処理には数分かかることがあります。次に、どのプラグインをインストールしたいかを尋ねられます。

  - すべてのプラグインをダウンロードするには「**All**」を選択します。
  - 「**1- Yes**」を選択して自環境で使用可能なプラグインをインストールします。

- ダウンロードにデフォルトのパスを使う場合は [Enter] キーを押します。
- Apache を自動設定（オプション）させるには「**2- No**」を選択します。
- Tomcat にデフォルトポート（8080）を承認します。

- Tomcat にデフォルト SSL ポート（8443）を承認します。
- Tomcat にデフォルト JK コネクタポート（9009）を承認します。
- 適切な管理権限を持つ管理ユーザの ID（たとえば「root.fts」）を入力してください。
- 適切な管理権限を持つ管理ユーザの ツリー名（たとえば「fwlab」）を入力してください。
- 「**1-OK...**」と一緒に表示されたエントリの要約を承認してインストールを終了させせます。

Novell iManager へのログイン

インストールが終わると、以下の URL からウェブブラウザ経由で iManager にログインできます。

https://<IP address of the eDirectory server>:8443/nps

Novell のブラウザには Microsoft Internet Explorer または Mozilla Firefox を推奨します。Mozilla Firefox の場合、一度にすべてのコンテキストメニューのポップアップウィンドウを表示させないようにすることもできます。

ConsoleOne のインストールと起動

ConsoleOne は Novell _eDirectory のもう 1 つの管理ツールです。

ConsoleOne を以下のようにインストールしてください。

▶ ルート権限（スーパーユーザ）で eDirectory Server にログインします。

▶ ディレクトリ **/home/eDirectory** に移動します。

```
cd /home/eDirectory
```

▶ ConsoleOne のアーカイブ **c1_136f-linux.tar.gz** を解凍します。

```
tar -xzvf c1_136f-linux.tar.gz
```

解凍すると、**/home/eDirectory** に **Linux** という新しいサブディレクトリが作られます。

▶ ディレクトリ **Linux** に進みます。

```
cd Linux
```

▶ インストール用スクリプト **c1-install** を呼び出します。

```
./c1-install
```

▶ インストール時のメッセージを出力する言語を選択します。

▶ 「8」を入力してすべてのスナップインをインストールしてください。

ConsoleOne にはインストール済みの Java ランタイム環境へのパスが必要です。対応するパス名を環境変数 **C1_JRE_HOME** にエクスポートすることができます。ただし、パス名をシステム全体にエクスポートするためには、**bash** プロファイルの変更が必要です。

i ConsoleOne を操作するためには、原則として ID「**superuser Root**」をエクスポートできるレベルのルート権限が要求されます。パス名をシステム全体にエクスポートする方法は以下に紹介する通りです。すなわち、通常のユーザでもルート権限があれば ConsoleOne を操作することができます。

次の手順に従います。

▶ 編集する設定ファイルを開きます（この例では「**/etc/bash.bashrc**」）。

▶ 設定ファイルの「# End of ...」の前に次の行を入力します。

```
export C1_JRE_HOME=/opt/novell/j2sdk1.4.2_05/jre
```

> i eDirectory と同時にインストールされた java ランタイム環境をここで使用します。一方、eDirectory Server 上にインストールされたいずれかの Java ランタイム環境のパス名を指定することもできます。

ConsoleOne はローカルの設定ファイル **hosts.nds** または SLP サービスとマルチキャストを経由して使用可能なツリー階層を取得します。

以下のように、ユーザのツリー階層を設定ファイルに挿入してください。

▶ 設定用ディレクトリに移動します。

```
cd /etc
```

▶ ファイル **hosts.nds** がまだ存在しない場合には作成してください。

▶ ファイル **hosts.nds** を開いて以下の行を挿入します。

```
#Syntax: TREENAME.FQDN:PORT
MY_Tree.mycomputer.mydomain:81
```

ConsoleOne の起動

ConsoleOne はシステムプロンプトから以下のコマンドを使用して起動できます。

```
/usr/ConsoleOne/bin/ConsoleOne
```

8.2.6.3 Novell eDirectory の設定

以下の手順を実行して Novell eDirectory を設定してください。

1. NDS ツリーを作成します。
2. eDirectory の LDAP 用設定
3. LDAP Browser を経由した eDirectory への試験アクセス

NDS ツリーの作成

ユーティリティ ndsmanage を使用して **NDS**（**N**etwork **D**irectory **S**ervice : ネットワークディレクトリサービス）ツリーを作成します。このためには、ndsmanage で以下の情報が必要になります。

ツリー名
: 新しい NDS ツリーのネットワーク用の一意の名前、たとえば「**MY_TREE**」。

サーバ名
: eDirectory 内の「**server**」クラスのインスタンス名。「**Server Name**」には、LDAP サーバが稼働している PRIMERGY サーバの名前を指定してください。たとえば、**lin36-root-0** と指定します。

サーバコンテキスト
: **server** オブジェクトを格納するコンテナの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、**dc=organization.dc=mycompany**。

Admin ユーザ
: 管理を実行する許可を持つユーザの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、**cn=admin.dc=organization.dc=mycompany**。

NCP ポート
: ポート 81 を指定してください。

インスタンスのロケーション
: 次のパスを指定します : **/home/root/instance0**

設定ファイル
: 次のファイルを指定します : **/home/root /instance0/ndsconf**

Admin ユーザのパスワード
: 管理者のパスワードをここに入力します。

次の手順で NDS ツリーを設定します。

► コマンドボックスを開きます。

► ディレクトリ **/home/eDirectory** に移動します。

► コマンド ndsmanage を入力してユーティリティ **ndsmanage** を起動します。

```
ndsmanage
```

► 「c」を入力して、クラス **server** の新しいインスタンスを生成します。

► 「y」を入力して設定作業を続けます。

► 「y」を入力して新しいツリーを作成します。

次に ndsmanage は、**TREE NAME**、**Server Name**、**Server Context** などの値を順に問い合わせます（261 ページを参照）。

入力が完了すると、NDS ツリーが ndsmanage によって設定されます。

► NDS ツリーの設定が終わったら、PRIMERGY サーバを再起動させて、設定の実効化、すなわち、NDS ツリーの再作成を行います。

LDAP 用の eDirectory の設定

eDirectory を LDAP 用に設定する手順は次の通りです。

– Role Based Services（RBS）をインストールします。

– プラグインモジュールの設定

– Role Based Services（RBS）の設定

– eDirectory の設定（SSL/TLS を使用する、もしくは使用しない）

以下の手順で個々の作業を完了させます。

► Web ブラウザを使用して、管理者 ID（**Admin**）で iManager にログインします。

Role Based Services（RBS）のインストール

iManager Configuration ウィザードを使用して RBS をインストールします。

次の手順に従います。

- ► iManager で、「**Configure**」タブを選択します（机のアイコンをクリックしてください）。
- ► 「**Configure**」タブで、次の順に選択します。
  「**Role Based Services**」- 「**RBS Configuration**」
- ► RBS Configuration ウィザードを起動します。
- ► 管理を行うコンテナに **RBS2** を割り当てます。（上の例では「mycompany"」となっています。）

プラグインモジュールのインストール

次の手順に従います。

- ► iManager で、「**Configure**」タブを選択します（机のアイコンをクリックしてください）。
- ► 「**Configure**」タブで、次の順に選択します。
  「**Plug-in installation**」- 「**Available Novell Plug-in Modules**」
- ► 「**Available Novell Plug-in Modules**」ページにリストされたモジュールから、eDirectory 専用のパッケージ **eDir_88_iMan26_Plugins.npm** を選択します。
- ► 「**インストール**」をクリックします。

Role Based Services（RBS）を設定します。

- ► 「**Available Novell Plug-in Modules**」ページで、LDAP 統合に必要なすべてのモジュールを選択してください。よくわからない場合は、すべてのモジュールを選択します。
- ► 「**インストール**」をクリックします。

eDirectory の SSL/TLS- セキュリティ保護されたアクセスの設定

i eDirectory のインストール中には、臨時の証明書が生成されますので、eDirectory へのアクセスは初期設定でも SSL/TLS によりセキュリティ保護されます。ただし、iRMC S4 のファームウェアは RSA/MD5 証明書を使用するように設定されているので、SSL/TLS セキュリティ保護された eDirectory 経由のグローバル iRMC S4 ユーザ管理には 1024 バイト長の RSA/MD5 証明書が必要です。

1024 バイト長の RSA/MD5 証明書は ConsoleOne を使用して以下のように作成します。

► 管理者 ID（**Admin**）を使用して LDAP サーバにログインし、ConsoleOne を起動してください。

► 社内ストラクチャのルートディレクトリに移動します（たとえば、**treename/mycompany/myorganisation**）。

► 「**New Object - NDSPKI key material - custom**」を選択して、クラス **NDSPKI:Key Material** の新しいオブジェクトを作成します。

► その後に表示されるダイアログで、以下の値を指定してください。

1. 1024 ビット
2. SSL または TLS
3. 署名 RSA/MD5

要求したタイプの署名が新しく作成されます。

新たに作成した証明書を SSL セキュリティ保護された LDAP 接続のために有効化するには、iManager で以下の作業を行います。

► ウェブブラウザから iManager を起動します。

► 有効な認証データを使用して iManager にログインします。

► **「LDAP」-「LDAP Options」-「LDAP Server」-「Connection」**の順に選択します。

「**Connection**」タブには、システム上でインストールされたすべての証明書を表示するドロップダウンリストがあります。

► ドロップダウンリストから必要な証明書を選択します。

eDirectory の SSL- セキュリティ保護されないアクセスの設定

eDirectory のデフォルト設定では匿名ログインやセキュリティ保護されないチャンネルを経由する平文表示のパスワードは無効となります。このため、eDirectory サーバにウェブブラウザでログインするには SSL 接続経由とするほかには方法がありません。

LDAP を SSL なしで使用したい場合は、以下の手順を実行しなければなりません。

1. SSL セキュリティ保護されない LDAP 接続の確立

2. バインド制限の緩和

3. LDAP 設定の再ロード

次の手順に従います。

1. SSL セキュリティ保護されない LDAP 接続の確立
   - ► ウェブブラウザから iManager を起動します。
   - ► 有効な認証データを使用して iManager にログインします。
   - ► 「**Roles and Tasks**」ビューを選択します。
   - ► **「LDAP」-「LDAP Options」-「LDAP Server」-「Connection」**の順に選択します。
   - ► 「**Connection**」タブで、以下のオプションを無効にします。
     Require TLS for all Operations
   - ► **「LDAP」-「LDAP Options」-「LDAP Group」-「General」**の順に選択します。
   - ► 「**General**」タブで、「**Require TLS for Simple Binds with password**」オプションを無効にします。
2. バインド制限の緩和
   - ► 有効な認証データを使用して iManager にログインします。
   - ► オブジェクトツリーで、**LDAP Server** オブジェクトに移動します。
   - ► マウスで **LDAP Server** オブジェクトをクリックしてハイライトさせ、関連するコンテキストメニューから「**Modify Object**」を選択します。
   - ► 右側のコンテントフレームで、「**Other**」シートを開きます。
   - ► 「**Valued Attributes**」で **ldapBindRestrictions** を選択します。
   - ► 「**編集**」ボタンをクリックします。
   - ► 値を「0」に設定します。
   - ► 「**OK**」をクリックします。
   - ► 「**Other**」シートで、「**適用**」ボタンをクリックします。
3. LDAP 設定の再ロード
   - ► ConsoleOne を起動して eDirectory にログインします。
   - ► ウィンドウの左側にある **Base DN** オブジェクト（たとえば **Mycompany**）をクリックします。すると、**LDAP server** オブジェクトがウィンドウの右側に表示されます。

- ▶ 右クリックして **LDAP Server** オブジェクトをハイライトさせ、関連するコンテキストメニューから「**Properties**」を選択します。
- ▶ 「**General**」タブで、「**Refresh NLDAP Server Now**」をクリックします。

LDAP ブラウザでの eDirectory アクセス試験

以上 1 から 3 までの手順に成功したら、LDAP ブラウザユーティリティを使用して eDirectory への接続が確立しなければなりません。Jarek Gavor 氏の LDAP ブラウザ（283 ページを参照）を使用して、以下のようにこの接続の試験をします。

▶ 管理者 ID

（たとえば **admin**）を使用して SSL 接続で eDirectory にログインできるか試してみます。

この接続に失敗した場合は、以下のようにしてください。

▶ SSL が有効であることを確認します（264 ページを参照）。

図 79: eDirectory への LDAP 接続の試験：SSL 有効時

▶ 管理者 ID

（たとえば **admin**）を使用して非 SSL セキュア接続で eDirectory にログインできるか試してみます。

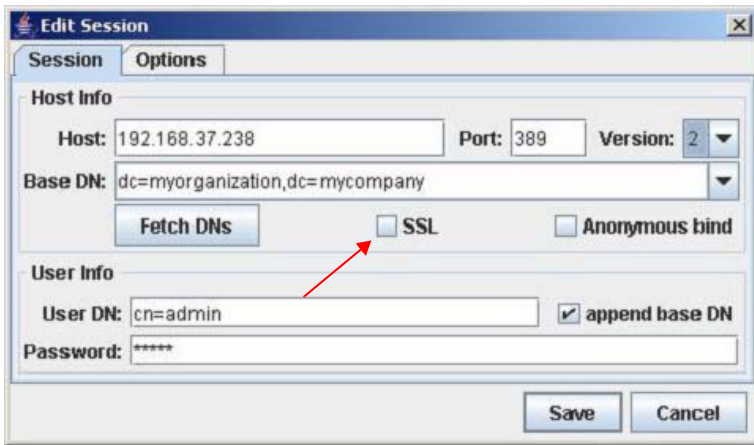



図 80: eDirectory への LDAP 接続の試験：SSL 無効時

▶ ログインが再度失敗する場合は、
バインド制限の緩和（264 ページを参照）。

8.2.6.4 iRMC S2/S3 ユーザ管理の Novell eDirectory への統合

前提条件：

LDAP v2 ストラクチャが eDirectory ディレクトリサービスですでに生成されていること（233 ページ の「SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除」の項を参照）。

以下の手順を実行して、iRMC S4 ユーザ管理を Novell eDirectory に統合します。

– iRMC プリンシパルユーザの作成

– eDirectory の iRMC グループとユーザ権限の宣言

– ユーザの許可グループへの割り当て

eDirectory の iRMC S4 LDAP ユーザ LDAP 認証プロセス

グローバル iRMC S4 ユーザが iRMC S4 にログインする際の認証は、定義済みのプロセスに従って処理されます（220 ページを参照）。268 ページ の図 81 では、この認証プロセスを、Novell eDirectory のグローバル iRMC S4 ユーザ管理に関して図解します。

対応するログイン情報による接続とログインの確立を、BIND 操作と呼びます。

1) iRMC S4 は､｢Principal User｣という定義済みで既知のアクセス許可データ（iRMC S4 設定）を使用して eDirectory サーバにログインし､正しくバインドされるのを待ちます。

2) iRMC S4 は eDirectory サーバに｢cn=User1｣でユーザの完全修飾識別された識別名（DN）を提供するようにリクエストします。eDirectory は定義済みのサブツリー（iRMC S4 設定）から DN を決定します。

3) iRMC S4 はユーザ User1 の完全修飾 DN を使用して eDirectory サーバにログインし、正常にバインドされるのを待ちます。

4) iRMC S4 は eDirectory サーバにユーザ User1 のユーザ権限を付与するようにリクエストします。

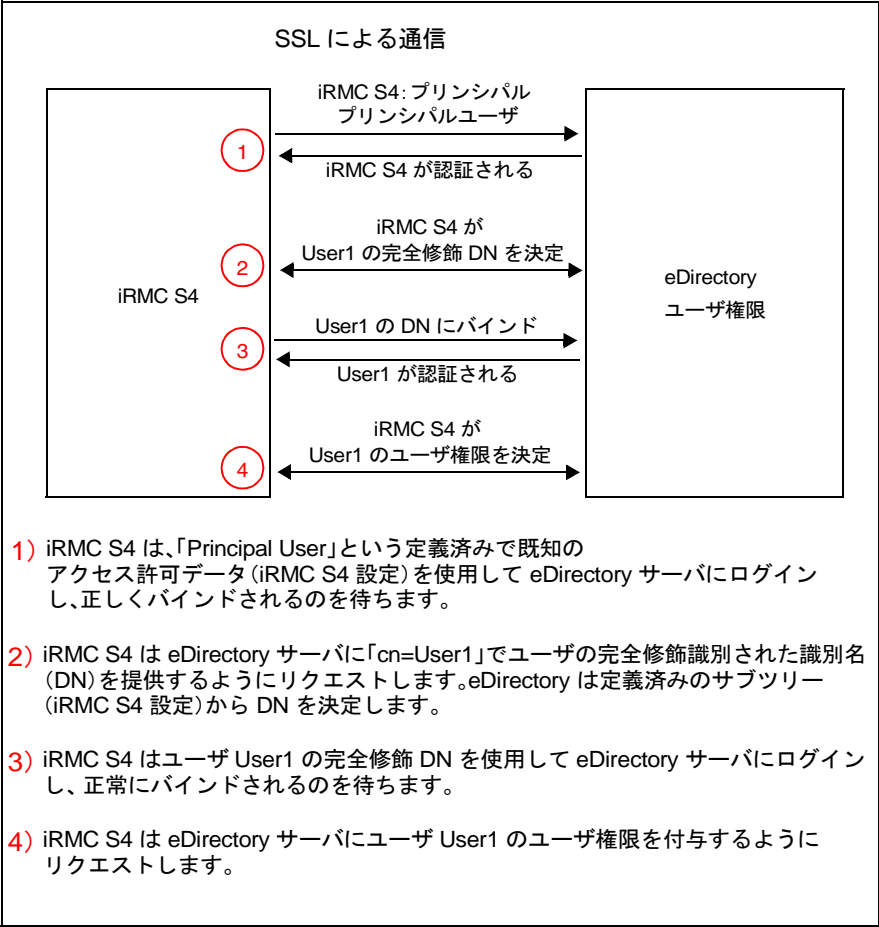



図 81: グローバル iRMC S4 権限の認証ダイアグラム

> **i** 「プリンシパルユーザ」権限データと DN を含むサブツリーは、iRMC S4 の Web インターフェースの「**Directory Service Configuration**」ページで設定します（マニュアル『iRMC S4 - integrated Remote Management Controller』を参照）。

> **i** ユーザの CN は、検索されるサブツリーの中で一意でなければなりません。

iRMC S4 用のプリンシパルユーザの作成

iRMC S4 用のプリンシパルユーザを以下の通り作成します。

- ▶ 有効な認証データを使用して iManager にログインします。
- ▶ 「**Roles and Tasks**」を選択します。
- ▶ 「**Users - Create User**」を選択します。
- ▶ 表示されるテンプレートに必要な項目を入力します。

  > **i** プリンシパルユーザの識別名（DN）とパスワードは対応する iRMC S4 の設定の項目に一致する必要があります（マニュアル『iRMC S4 - integrated Remote Management Controller』を参照）。
  >
  > ユーザの「**Context:**」はツリーのどの位置にあっても構いません。

- ▶ 以下のサブツリーにプリンシパルユーザの検索許可を割り当てます。
  - – サブツリー（OU）**SVS**
  - – ユーザを含むサブツリー（OU）（たとえば「**people**」）

iRMC グループとユーザへのユーザ権限の割り当て

デフォルト設定では、eDirectory のオブジェクトには、LDAP ツリー内の非常に限定されたクエリと検索の許可しかありません。ひとつまたは複数のサブツリーのすべての属性をオブジェクトがクエリできるようにするには、このオブジェクトに対応する許可を割り当てる必要があります。

許可は個々のオブジェクト（すなわち個々のユーザ）に割り当てることもできますし、同じ組織単位（OU）の中で照合されるオブジェクトのグループ（「**SVS**」または **people**。この場合、OU に割り当てられ、「引き継がれた」と識別された許可は、このグループのオブジェクトに自動的に認定されます。

i iRMC S4 ユーザ管理と Novell eDirectory を統合するには、次のオブジェクト（トラスティ）に検索の許可を割り当てる必要があります。

– **プリンシパルユーザ**
– iRMC S4 ユーザが含まれるサブツリー

以下にこの操作を詳しく説明します。

すべての属性に関するオブジェクト検索許可を割り当てるプロセスは以下の通りです。

▶ ウェブブラウザから iManager を起動します。

▶ 有効な認証データを使用して iManager にログインします。

▶ iManager で、「**Roles and Tasks**」ボタンをクリックします。

▶ メニューツリーストラクチャで、「**Rights**」-「**Rights to Other Objects**」の順に選択します。

「**Rights to Other Objects**」ページが表示されます。

▶ 「**Trustee Name**」の下に、アクセス許可を許可するオブジェクトの名前を指定します（271 ページ の図 82 の「**SVS.sbdr4**」)。

▶ 「**Context to Search From**」で、eDirectory のサブツリー（**SVS**）を指定します。iManager ははこのサブツリーから、トラスティ「**Users**」が現在読み取りの許可を持っているオブジェクトを検索します。

▶ 「**OK**」をクリックします。

進捗ディスプレイに検索の状況が表示されます。検索作業か終了すると、「**Rights to Other Objects**」ページに検索結果が表示されます（271 ページ の図 82 を参照）。

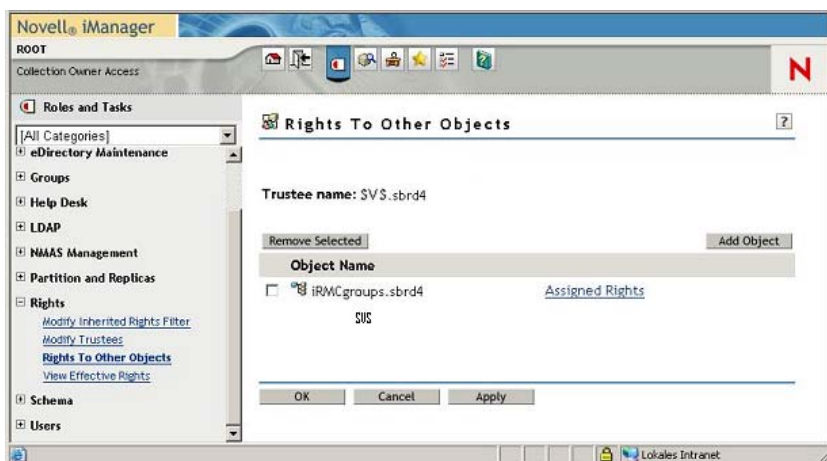



図 82: iManager - ロールとタスク - 他のオブジェクトに対する権限

「**Object Name**」の下に何もオブジェクトが表示されない場合、トラスティには指定されたコンテキストの範囲内に許可はありません。

► 必要に応じてトラスティに追加の許可を割り当ててください。

- ► 「**Add Object**」をクリックします。
- ► オブジェクトセレクタボタンを使用して、 トラスティに許可を割り当てたいオブジェクトを選択します。
- ► 「**Assigned Rights**」をクリックします。

  プロパティ「**All Attributes Rights**」が表示されない場合 :

  - ► 「**Add Property**」をクリックします。

    「**Add Property**」ウィンドウが表示されます（272 ページ の図 83 を参照）。

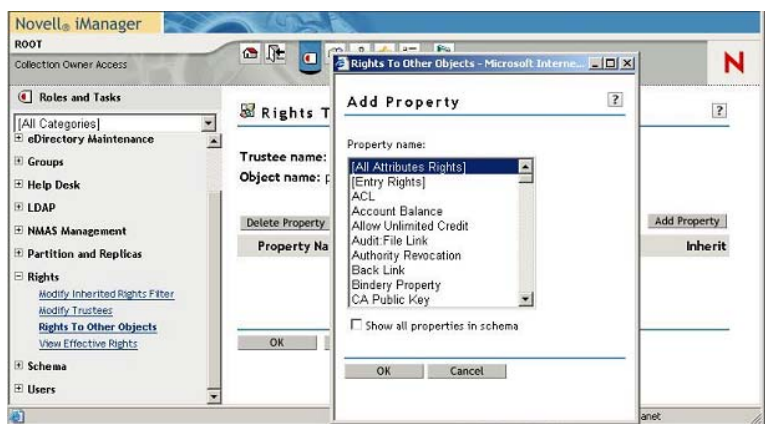



図 83: iManager - ロールとタスク - 他のオブジェクトに対する権限？プロパティの追加

► プロパティ「**All Attributes Rights**」をハイライトさせ、「**OK**」をクリックして追加します。

► プロパティ「**All Attributes Rights**」に対し、オプション「**Compare**」、「**Read**」、「**Inherit**」を有効にし、「**OK**」をクリックして確定します。

この操作によって、ユーザまたはユーザグループに、選択されたオブジェクトのサブツリーの属性をすべてクエリする権限が与えられます。

► 「**適用**」をクリックして、設定を有効にします。

8.2.6.5 iRMC S4 ユーザの許可グループへの割り当て

iRMC S4 ユーザを（たとえば OU「**people**」から）次のいずれの方法でも iRMC 許可グループに割り当てる事ができます。

– ユーザエントリから開始（ユーザエントリの数がごく少ない場合はこの方が適当）
– または、ロールエントリ／グループエントリから開始（ユーザエントリの数が多い場合はこの方が適当）

i 次の例は iRMC S4 ユーザを OU「**people**」から許可グループに割り当てる方法を示します。割り当てをロールエントリ／グループエントリから開始する方法を説明しています。

ユーザエントリに基づく割り当て方法もほぼ同じです。

i eDirectory 内のグループにユーザを「手作業」で入力する必要があります。

次の手順に従います。

▶ ウェブブラウザから iManager を起動します。

▶ 有効な認証データを使用して iManager にログインします。

▶ 「**Roles and Tasks**」を選択します。

▶ 「**Groups - Modify Group**」を選択します。

「**Modify Group**」ページが表示されます。

▶ iRMC S4 ユーザを割り当てたいすべての許可グループについて次の作業を実行します。

▶ オブジェクトセレクタボタンを使用して、 iRMC S4 ユーザを追加したい許可グループを選択します。LDAP v2 ストラクチャの例（274 ページ の図 84 を参照）ではこの操作は、**Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4**。

► 「メンバ」タブを選択します。

「**Modify Group**」ページの「**Members**」タブが表示されます。

図 84: 「iManager」-「Roles and Tasks」-「Modify Group」-「Members」タブ（LDAP v2）

► iRMC グループに割り当てたい OU「**people**」のすべてのユーザについて、次の作業を実行します。

► オブジェクトセレクタボタンをクリックします。 と共に提供されます。

「**Object Selector**（**Browser**）」ウィンドウが開きます（275 ページ の図 85 を参照）。

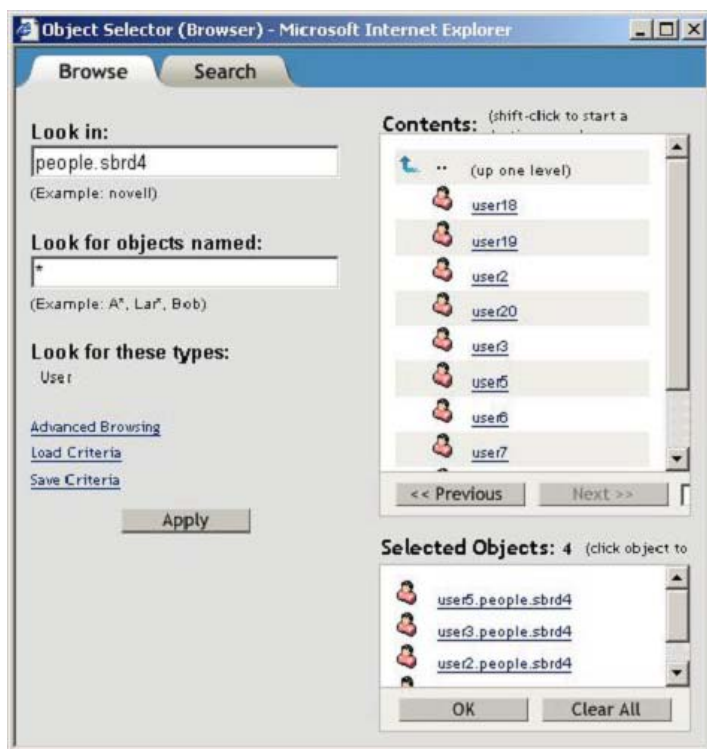



図 85: iRMC グループへのユーザの割り当て - ユーザの選択

► 「**Object Selector**（**Browser**）」ウィンドウで、OU「**people**」の中の必要なユーザを選択し、「**OK**」をクリックして確定します。

選択されたユーザは「**Modify Group**」ページの「**Members**」タブの表示領域にリストされています（274 ページ の図 84 を参照）。

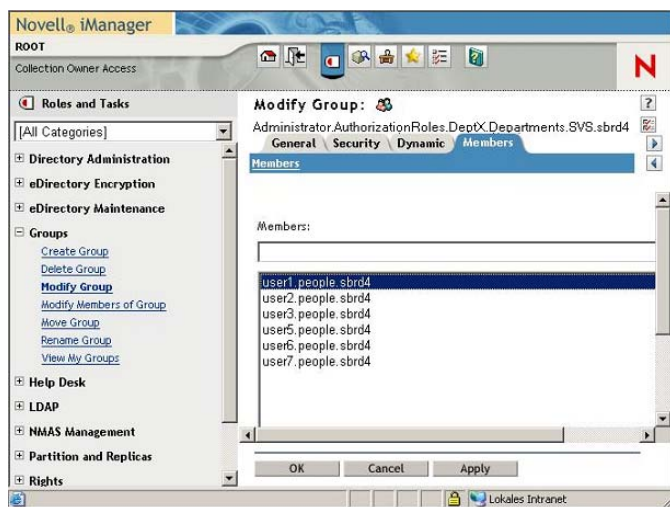



図 86: 「Members LDAP v2」タブが選択された iRMC S4 ユーザ表示

► 選択されたユーザが iRMC グループに追加されるように、「**Apply**」または「**OK**」で確定します（この例では **....SVS.sbdr4**）。

8.2.6.6 Novell eDirectory 管理のためのヒント

NDS デーモンの再起動

次の手順で NDS デーモンを再起動します。

▶ コマンドボックスを開きます。

▶ ルート許可でログインします。

▶ 次のコマンドを実行します。

```
rcndsd restart
```

nldap デーモンの再起動に失敗し、理由が分からない場合

▶ **nldap** デーモンを「手作業」で起動します。

```
/etc/init.d/nldap restart
```

iManager から応答がない場合

▶ iManager を再起動してください。

```
/etc/init.d/novell-tomcat4 restart
```

NLDAP サーバ設定の再ロード

次の手順に従います。

▶ ConsoleOne を起動して eDirectory にログインします。

ConsoleOne を初めて立ち上げる場合は、ツリーが設定されていません。

以下の手順でツリーを設定してください。

▶ 「**My World**」の下のノード「**NDS**」を選択します。

▶ メニューバーから「**File**」- 「**Authenticate**」の順に選択します。

▶ 次のログイン用認証データを入力します。

1. ログイン名：root
2. パスワード： <password>
3. ツリー : MY_TREE
4. コンテキスト：mycompany

► ウィンドウの左側部分で、「**Base DN**」オブジェクト（**Mycompany**）をクリックします。

すると、「**LDAP Server**」オブジェクトがウィンドウの右側に表示されます。

► 「**LDAP Server**」オブジェクトを右クリックし、コンテキストメニューで「**Properties**」を選択します。

► 「**General**」タブで、「**Refresh NLDAP Server Now**」ボタンをクリックします。

NDS メッセージトレースの設定

nds デーモンは、デバッグメッセージとログメッセージを生成します。このメッセージは **ndstrace** ツールを使用してトレースすることができます。以下に説明する設定の目的は、**ndstrace** からの出力をファイルにリダイレクトし、他のターミナルでこのファイルの内容を表示させることです。後者の作業には **screen** ツールを使用します。

以下の手順を推奨します。

► コマンドボックス（たとえば **bash**）を開きます。

ndstrace を設定します。

► eDirectory のディレクトリ **/home/eDirectory** に移動します。

```
cd /home/eDirectory
```

► `screen` コマンドを使用して **screen** を起動します。

► `ndstrace` コマンドを使用して **ndstrace** を起動します。

► 有効化したいモジュールを選択します。

たとえば、イベントが発生した時間を表示したい場合は、「`dstrace TIME`」と入力します。

LDAP および **TIME** モジュールを有効化するには、以下を入力することを強く推奨します。

```
dstrace LDAP TIME
```

► **quit** と入力して **ndstrace** を終了します。

これで **ndstrace** の設定は終了しました。

別のターミナルでのメッセージの出力

▶ **ndstrace** を起動して、メッセージ出力をリダイレクトします。

```
ndstrace -l >ndstrace.log
```

▶ 以下のキーの組み合わせを使用して別のターミナルを開きます。
[Ctrl] + [[a]]、Ctrl + [c]

▶ ログの記録を開始します。

```
tail -f ./ndstrace.log
```

▶ 仮想端末を切り替えるには、キーの組み合わせ [Ctrl] + [a]、[Ctrl] + [0] を使用します。
（ターミナルには 0 から 9 までの番号が付きます。）

8.2.7 OpenLDAP による iRMC S4 ユーザの管理

この節では次の点について説明します。

– OpenLDAP（Linux）のインストール
– SSL 証明書の作成
– OpenLDAP の設定。
– iRMC S4 ユーザの管理の OpenLDAP への統合
– OpenLDAP 管理のヒント

8.2.7.1 OpenLDAP のインストール

i OpenLDAP をインストールする前に、ファイヤーウォールをポート 389 と 636 に接続できるように設定する必要があります。

OpenSuSE の場合は以下の手順に従います。

► ファイル **/etc/sysconfig/SuSEfirewall2** で、オプション **FW_SERVICES_EXT_TCP** を次のように拡張します。

```
FW_SERVICES_EXT_TCP=“389 636”
```

配布媒体から取得したパッケージ **OpenSSL** および **OpenLDAP2** をインストールするときは、セットアップツール YaST を使用してください。

8.2.7.2 SSL 証明書の作成

次のプロパティを持つ証明書を作成する必要があります。

– 鍵の長さ : 1024 ビット
– md5RSAEnc

鍵ペアと署名入り証明書（自己署名または外部 CA の署名）の作成には OpenSSL を使用します。より詳しい情報は OpenSSL のホームページ、*http://www.openssl.org* を参照してください。

CA の設定とテスト証明書の作成の説明書は以下のリンクから入手してください。

– *http://www.akadia.com/services/ssh_test_certificate.html*
– *http://www.freebsdmadeeasy.com/tutorials/web-server/apache-ssl-certs.php*
– *http://www.flatmtn.com/computer/Linux-SSLCertificates.html*
– *http://www.tc.umn.edu/~brams006/selfsign.html*

証明書の作成に続いて、以下の 3 個の PEM ファイルを入手してください。

– ルート証明書 : **root.cer.pem**

– サーバ証明書 : **server.cer.pem**

– 秘密鍵 : **server.key.pem**

> **i** 秘密鍵は決してパスフレーズで暗号化**しないでください。**
> **server.key.pem** ファイルには、LDAP デーモン（**ldap**）読み取り許可**のみが割り当てられる**ためです。
>
> 次のコマンドを使用してパスフレーズを削除してください。
>
> ```
> openssl rsa -in server.enc.key.pem -out server.key.pem
> ```

8.2.7.3 OpenLDAP の設定

次の手順で OpenLDAP を設定します。

► Yast セットアップツールを起動させ、「**LDAP-Server-Configuration**」を選択します。

► 「**Global Settings/Allow Settings**」で **LDAPv2-Bind** の設定を有効にします。

► 「**Global Settings/TLS Settings**」を選択します。

  ► **TLS** 設定を有効にします。

  ► インストール時に作成されたファイルのパスを宣言してください（280 ページ の「OpenLDAP のインストール」の項 を参照）。

  ► ファイルシステムの証明書と秘密鍵を読み取ることができるのは LDAP サービスのみであることを確認してください。

  openldap は **uid/guid=ldap** の下で実行されるので、確認は以下の方法で行うことができます。

  – ファイルのオーナーの証明書と秘密鍵を「ldap」に設定する

  – または、LDAP デーモン **ldap** の読み取り許可を証明書と秘密鍵が入ったファイルに割り当てる

► 「**Databases**」を選択して新しいデータベースを作成します。

i YaST で作成した設定が全体的に機能しない場合には、以下の必須エントリがファイル **/etc/openldap/slapd.conf** にあるかを確認してください。

```
allow bind_v2
```

```
TLSCACertificateFile /path/to/ca-certificate.pem
```

```
TLSCertificateFile /path/to/certificate.pem
```

```
TLSCertificateKeyFile /path/to/privat.key.pem
```

i YaST で作成した SSL の設定が機能しない場合は、以下のエントリが設定ファイル **/etc/sysconfig/openldap** にあるかを確認してください。

```
OPENLDAP_START_LDAPS=“yes”
```

8.2.7.4 iRMC S2/S3 ユーザの管理の OpenLDAP への統合

前提条件：

LDAP v2 ストラクチャが OpenLDAP ディレクトリサービスのなかに生成済みであること（233 ページ の「SVS_LdapDeployer - 「SVS」ストラクチャの生成、保守および削除」の項を参照）。

iRMC S4 ユーザ管理の OpenLDAP への統合は以下の手順で行います。

– iRMC プリンシパルユーザの作成

– 新規 iRMC S4 ユーザの作成とそのユーザに対する許可グループの割り当て

プリンシパルユーザ（ObjectClass : **Person**）を作成するには、Jarek Gawor 氏作の LDAP Browser\Editor などの LDAP ブラウザ（283 ページ を参照）を使用します。

Jarek Gawor 氏の著作による LDAP Browser\Editor

Jarek Gawor 氏の著作による LDAP Browser\Editor はグラフィカルユーザインターフェースによる使いやすいものです。

このツールはインターネットでダウンロードできます。

以下の手順で **LDAP Browser\Editor をインストール**してください。

► 圧縮アーカイブ **Browser281.zip** を任意のインストール用ディレクトリで解凍します。

► JAVA ランタイム環境用の環境変数 **JAVA_HOME** をインストール用ディレクトリに設定します。たとえば、以下のようにします。

```
JAVA_HOME=C:\Program Files\Java\jre7
```

プリンシパルユーザの作成

プリンシパルユーザ（ObjectClass : **Person**）を作成するには、Jarek Gawor 氏作の LDAP Browser\Editor などの LDAP ブラウザ（283 ページ を参照）を使用します。

以下に、Jarek Gawor 氏の LDAP Browser\Editor を用いてプリンシパルユーザを作成する方法を説明します。

次の手順に従います。

- ► LDAP ブラウザを起動します。
- ► 有効な認証データを使用して OpenLDAP ディレクトリサービスにログインします。
- ► プリンシパルユーザを作成するサブツリー（サブグループ）を選択します。プリンシパルユーザはサブツリー内のどこにでも作成できます。
- ► 「**編集**」メニューを開きます。
- ► 「**Add Entry**」を選択します。
- ► 「**Person**」を選択します。
- ► 識別名 **DN** を編集します。

  プリンシパルユーザの識別名（DN）とパスワードは対応する iRMC S4 の設定の項目に一致する必要があります（マニュアル『iRMC S4 - integrated Remote Management Controller』を参照）。

- ► 「**Set**」をクリックしてパスワードを入力します。
- ► 苗字 **SN** を入力します。
- ► 「**Apply**」をクリックします。

新規 iRMC S2/S3 ユーザの作成とそのユーザに対する許可グループの割り当て

i 新規ユーザ（ObjectClass **Person**）の作成とユーザの許可グループへの割り当てには、LDAP ブラウザ、たとえば Jarek Gawor 氏が作成した LDAP Browser\Editor などを使用します（283 ページを参照）。

以下に、Jarek Gawor 氏の LDAP Browser\Editor を用いて新規の iRMC S4 ユーザを作成し、そのユーザを許可グループに割り当てる方法を説明します。

次の手順に従います。

▶ LDAP ブラウザを起動します。

▶ 有効な認証データを使用して OpenLDAP ディレクトリサービスにログインします。

▶ 新規ユーザを作成します。

これは次の手順で行います。

- ▶ 新規ユーザを作成するサブツリー（サブグループ）を選択してください。新規ユーザはサブツリー内のどこにでも作成できます
- ▶ 「**編集**」メニューを開きます。
- ▶ 「**Add Entry**」を選択します。
- ▶ 「**Person**」を選択します。
- ▶ 識別名 **DN** を編集します。
- ▶ 「**Set**」をクリックしてパスワードを入力します。
- ▶ 苗字 **SN** を入力します。
- ▶ 「**Apply**」をクリックします。

► 今作成したユーザを許可グループに割り当てます。

これは次の手順で行います。

► ユーザを所属させる **SVS** サブツリー（サブグループ）を次のように選択します。

cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

► 「**編集**」メニューを開きます。

► 「**Add Attribute**」を選択します。

► 属性名として「Member」を指定します。値にはここで作成したユーザの完全修飾 DN を次のように指定してください。

cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS, dc=myorganisation,dc=mycompany

8.2.7.5 OpenLDAP 管理のヒント

LDAP サービスの再起動

次の手順で LDAP サービスを再起動します。

▶ コマンドボックスを開きます。

▶ ルート許可でログインします。

▶ 次のコマンドを入力します。

```
rcldap restart
```

メッセージログの記録

LDAP デーモンは Syslog プロトコルを使用してメッセージログを記録します。

記録されたメッセージは、ファイル **/etc/openldap/slapd.conf** でログレベルが 0 以外に設定されている場合にのみ表示されます。

各レベルの説明は下記を参照してください。

http://www.zytrax.com/books/ldap/ch6/#loglevel

288 ページ の表 37 に、ログレベルとその意味の概要を記載しています。

ログレベル	意味
-1	全面的なデバッグ実行
0	デバッグ実行なし
1	ログファンクションコール
2	試験パケットの取扱い
4	ヘビートレースデバッグ実行
8	接続管理
16	送信 / 受信パケット表示
32	フィルタ処理の検索
64	設定ファイル処理
128	アクセス制御リスト処理
256	接続／操作／イベントのステータスログの記録
512	送信済みエントリのステータスログの記録
1024	シェルバックエンドによる出力通信
2048	エントリパースの出力結果

表 37: OpenLDAP - ログレベル

8.2.8 グローバル iRMC S4 ユーザ宛ての Email 警告の設定

グローバル iRMC S4 ユーザ宛の Email 警告が、グローバル iRMC S4 ユーザ管理システムに組み込まれています。すなわち、1 台のディレクトリサーバを使用して、Email 警告をすべてのプラットフォーム向けに集中的に設定し操作することができます。適切に設定されたグローバルユーザ ID は、ネットワーク上でディレクトリサーバに接続されたすべての iRMC S4 から Email 警告を受け取ることができます。

前提条件

Email 警告には、以下の要件を満たす必要があります。

– グローバル Email 警告には、LDAP v2 のストラクチャとしてバージョン 3.77A 以降の iRMC S4 ファームウェアが必要です。

– プリンシパルユーザが iRMC S4 Web インターフェースで設定され、LDAP ツリー内で検索する権限が付与されているる必要があります（マニュアル『iRMC S4 - integrated Remote Management Controller』を参照）。

– LDAP 設定を「**ディレクトリサービス構成**」ページで設定する際（マニュアル『iRMC S4 - integrated Remote Management Controller』を参照）、E-mail 設定を「**ディレクトリサービス E-mail 警告構成**」で有効にしておく必要があります。

8.2.8.1 グローバル Email 警告

ディレクトリサーバ経由のグローバル Email 警告には警告ロールが必要です。この警告ロールは管理ロールに加えて **SVS_LdapDeployer** の設定ファイル（233 ページを参照）で定義されます。

警告グループ（警告ロール）の表示

警告ロールは警告タイプ（たとえば、温度のしきい値を超えた、など）をまとめてグループ化しますが、それぞれに重要度（たとえば「致命的」）が割り当てられています。ユーザを特定の警告グループに割り当てると、ユーザが Email で受け取る警告のタイプと重大度が指定されます。

警告ロールの構文はサンプル設定ファイル **Generic_Settings.xml** と **Generic_InitialDeploy.xml** に具体的に解説されています。これらのファイルは、ServerView Suite DVD 1 に収録される **jar** アーカイブ **SVS_LdapDeployer.jar** に付属しています。

警告タイプの表示

以下の警告タイプがサポートされます。

警告タイプ	原因
FanSens	冷却ファンセンサ
Temperat	温度センサ
HWError	致命的なハードウェア故障
セキュリティの設定	セキュリティの設定
SysHang	システムのハング
POSTErr	POST エラー
SysStat	システムステータス
DDCtrl	ディスクドライブとコントローラ
NetInterf	ネットワークインターフェース
RemMgmt	リモートマネジメント
SysPwr	電源管理
メモリ	メモリ
その他	その他

表 38: 警告タイプ

各々の警告タイプには以下の重大度のいずれかが割り当てられます : **警告**、**致命的**、**すべて**、(**なし**)。

優先メールサーバ

グローバル Email 警告には、優先メールサーバの「**Automatic** 設定が適用されます。Email が即時に送ることができない場合、たとえば 1 番目のメールサーバが使用不可能な場合には、Email は 2 番目のメールサーバに送られます。

サポートされるメールフォーマット

以下の Email フォーマットがサポートされています。

– 標準
– 題名固定
– ITS フォーマット
– Fujitsu REMCS フォーマット

i **標準**以外のメールフォーマットを使用する場合は、対応するメールフォーマットグループにユーザを追加しなければなりません。

LDAP Email テーブル

Email 警告が設定され（292 ページを参照)、「**LDAP E-mail 通知を有効にする**」オプション（『iRMC S4 - integrated Remote Management Controller』マニュアルを参照）が選択されている場合は、iRMC S4 は警告が発行されると以下のユーザに Email を送信します。

– 適切に設定されたすべてのローカル iRMC S4 ユーザ

– この警告のための LDAP Email テーブルに登録されているすべての iRMC S4 ユーザ

LDAP Email テーブルは、iRMC S4 が初回に起動されたときに、iRMC S4 ファームウェアにより最初に作成され、定期的に更新されます。LDAP Email テーブルのサイズは、最大 64 の LDAP 警告ロールと、Email 警告の送信先に設定されている最大 64 のグローバル iRMC S4 ユーザに限定されています。

i グローバル Email 警告には Email 配布リストの使用を推奨します。

LDAP ディレクトリサーバは、Email 警告の目的で、以下の情報を Email テーブルから取得します。

- Email 警告が設定されたグローバル iRMC S4 ユーザのリスト
- 各グローバル iRMC S4 ユーザに対して：
  – 警告タイプ毎に設定された警告のリスト（タイプと重大度）
  – 要求されたメールフォーマット

LDAP Email テーブルは以下の状況で更新されます。

– iRMC S4 が初回に起動、または再起動されたとき

– LDAP の設定が変更されたとき

– 定期的（任意）更新の間隔は、iRMC S4 Web インターフェースでの LDAP 設定の一部として「**LDAP 警告テーブルを更新する**」オプションで指定します（マニュアル『iRMC S4 - integrated Remote Management Controller』および「**LDAP 警告テーブルを更新する**」オプションを参照）。

ディレクトリサーバ上のグローバル Email 警告の設定

この節ではディレクトリサーバ上に LDAP Email 警告を設定する方法を説明します。

i 設定は、iRMC S4 上にも行う必要があります。これは、iRMC S4 Web インターフェースで設定します（マニュアル『iRMC S4 - integrated Remote Management Controller』を参照）。

次の手順に従います。

► ディレクトリサービスに Email 警告を送信するユーザの Email アドレスを入力します。

  i Email アドレス設定に使用する方法は、運用するディレクトリサービス（Active Directory、eDirectory または OpenLDAP）によって異なります。

► 警告ロールを定義する設定ファイルを作成します。

► この設定ファイルを使用して **SVS_LdapDeployer** を起動し、対応する LDAP v2 ストラクチャ（**SVS**）をディレクトリサーバ上に生成させます（234 ページと 240 ページを参照）。

8.2.8.2 警告ロールの表示

LDAP v2 ストラクチャが生成されると、新たに作成された OU「**SVS**」が表示されます。たとえば、Active Directory では、**Declarations** の配下にコンポーネント **Alert Roles** および **Alert Types** と一緒に、また **DeptX** の配下にコンポーネント **Alert Roles** と一緒に表示されます（図 87 を参照）。

– **Declarations** の配下では、**Alert Roles** にすべての定義された警告ロールが表示され、**Alert Types** の下にすべての警告タイプが表示されます（1）。

– **DeptX** の配下では、**Alert Roles** の下に OU「**DeptX**」において有効なすべての警告ロールが表示されます（2）。

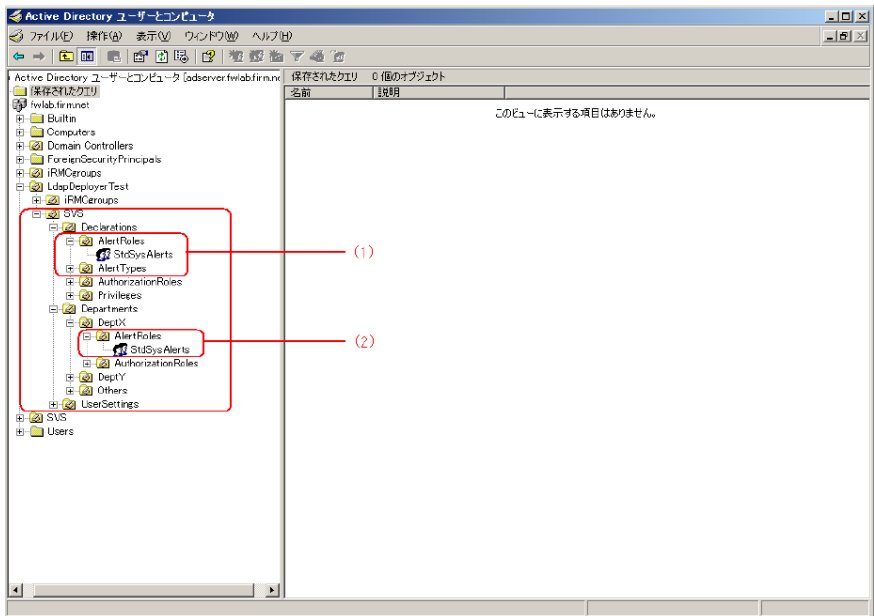



図 87: OU「SVS」と警告ロール

個々の警告ロールのユーザに Email が確実に送信されるようにするため、関連部門を iRMC S4 に設定する必要があります（図 87 の **DeptX**）（『iRMC S4 - integrated Remote Management Controller』マニュアルを参照）。

「Active Directory ユーザとコンピュータ」のストラクチャツリーで**「SVS」–「Departments」–「DeptX」–「Alert Roles」**の下にある警告ロール（たとえば**「StdSysAlerts」**）を選択し（図 88 を参照）（1）、コンテキストメニューから**「プロパティ」–「メンバ」**を選択して**「プロパティ」**ダイアログボックスを開くと、その警告ロール（この例では**「StdSysAlerts」**）が**「メンバ」**タブの中に表示されます（2）。

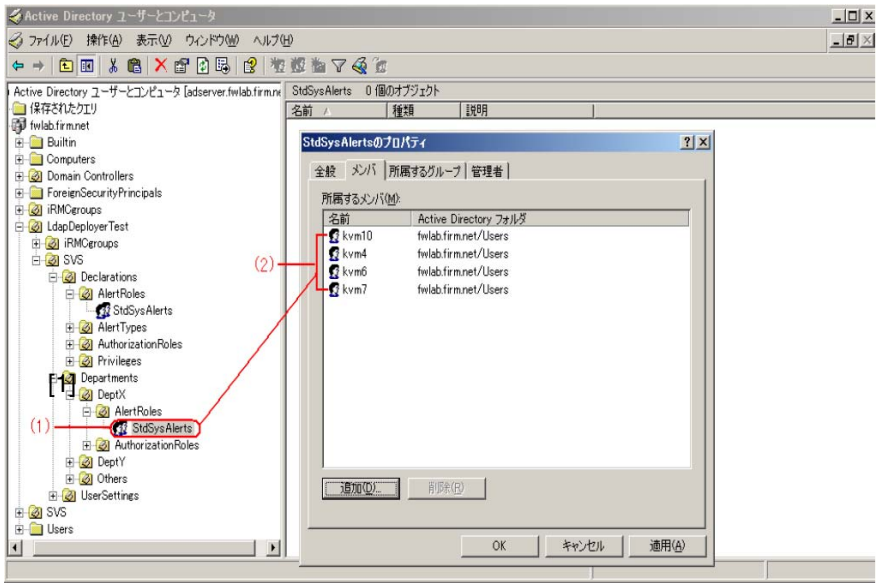



図 88: 警告ロール「StdSysAlert」に割り当てられたユーザ

8.2.8.3 iRMC S4 ユーザへの警告ロール割り当て

iRMC S4 ユーザに、以下のいずれかの方法で警告ロールを割り当てる事ができます。

– ユーザエントリに基づいて
– または、ロールエントリに基づいて

各種ディレクトリサービス（Microsoft Active Directory、Novell _eDirectory および OpenLDAP）において、iRMC S4 への 警告ロールの割り当ては、iRMC S4 ユーザへ権限ロール（Authorization roles）を割り当てられるのと同じ方法で、同じツールを使用して行われます。

たとえば、Active Directory の場合は、「**Active Directory ユーザとコンピュータ**」スナップインの「**プロパティ**」ダイアログボックスの中の「**追加**」をクリックして割り当てを行います。（294 ページ の図 88 を参照）

8.2.9 SSL copyright

iRMC S4-LDAP の統合には、OpenSSL プロジェクトに基づき Eric Young 氏が開発した SSL 実装を使用します。

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```